Examining Fifth Generation Messaging Systems

Michelle Mutu-Grigg
University of Auckland
New Zealand
smg@quicksilver.net.nz

31 January 2003

Abstract

Inherent in life is the need for communication. As time has passed communication methods and systems have expanded and developed. This paper examines a fifth generation messaging system proposed by Jihong Li in her Master's thesis *A fifth generation messaging system*. It discusses four problems identified in this thesis and then redefines and examines the "persona problem" or the identification and uses of a person's various "personalities" in a messaging system. This problem is refined and examined in the concept of persona identification.

To help provide understanding of this concept an electronic mailing system design that would be able to identify "persona" is discussed. A current graphical user interface electronic mailing system is examined before a user interface that could be integrated with a fifth generation messaging system is presented. This paper then discusses possible implementations of this persona concept through manipulation of existing filters and methods. Through this discussion the validity of the inclusion of persona identification features in a fifth generation system is established.

This paper also examines relevant models and literature that was not cited by Li in her thesis. The two key areas this paper examines are persona and presence awareness.

Name: Michelle Mutu-Grigg
Paper: CompSci 380AC 2003
ID: 9564814

Examining Fifth Generation Messaging Systems

Michelle Mutu-Grigg
University of Auckland
New Zealand
smg@quicksilver.net.nz

1. Abstract

Inherent in life is the need for communication. As time has passed communication methods and systems have expanded and developed. This paper examines a fifth generation messaging system proposed by Jihong Li in her Master's thesis *A fifth generation messaging system*. It discusses four problems identified in this thesis and then redefines and examines the "persona problem" or the identification and uses of a person's various "personalities" in a messaging system. This problem is refined and examined in the concept of persona identification.

To help provide understanding of this concept an electronic mailing system design that would be able to identify "persona" is discussed. A current graphical user interface electronic mailing system is examined before a user interface that could be integrated with a fifth generation messaging system is presented. This paper then discusses possible implementations of this persona concept through manipulation of existing filters and methods. Through this discussion the validity of the inclusion of persona identification features in a fifth generation system is established.

This paper also examines relevant models and literature that was not cited by Li in her thesis. The two key areas this paper examines are persona and presence awareness.

2. Introduction

2.1. Messaging systems

Throughout time clear communication between people has been a key element in society. Methods of communication have taken many shapes and forms. In today's society, efficient and effective messaging systems are a key component

to a successful business environment. These systems must allow a user flexibility of use and with the advent of convenient travel and must cater for the mobility today's work environment demands. With the development of various media types such as sound, digital images, and motion capture, they must have the ability to deal with varying types of data transfer. These systems must provide a service that will allow users to conduct communications in a high-speed, mobile and secure manner. To ensure usability these systems must also have the ability to be customised to a user's preference.

Over time different generations of messaging systems have developed. This paper examines systems to date and a fifth generation messaging system model proposed in Jihong Li's Master's thesis [Li, 2001]. It then looks at areas not examined in the thesis and suggests some improvements.

To help in the understanding of this model, problems with current messaging systems are discussed. Li's Masters thesis identified four problems. In addition to these problems this paper examines, designs and presents a graphical user interface for an electronic mailing system to demonstrate an implementation of the persona identification concept examined in Sections 3.2.3, 4 and 5. The following is a brief look at these four identified problems with messaging systems, summarized and redefined from Li's thesis.

2.2. Messaging system problems

2.2.1 Communication problem

As society has developed, so have the techniques used by people to send messages to each other, even if the recipient is at a large distance from the sender. For millennia, humans have used a variety of visual and audio techniques, such as drums and smoke signals, to communicate over distances.

Communications changed dramatically with the invention of the telephone by Alexander Graham Bell in 1876 [Cherry, 1953] enabling voice communications over significant land mass areas. From here methods of communication developed in leaps and bounds, from time-division multiplex and pulse modulation systems, to today's advanced globally linked networks.

Despite this extensive development in messaging systems, each person still encounters a “communication problem” whenever they are unable to send a message to someone else, in a rapid, convenient and inexpensive way.

2.2.2 Translation problem

As communication methods have developed the methods in which messages are sent and received have changed. With the development of different communication systems, people have encountered a “translation problem” whenever they wish to send a message from one type of device, to a recipient using another type of device.

With the recent proliferation of communication devices such as Personal Digital Assistants (PDAs), computers for electronic mail, and cellular phones, the “translation problem” has been partially addressed by the provision of various ad-hoc methods for translating messages from one format to another.
An example of a partial solution to the translation problem is the ability to pass messages effectively between the digital Integrated Services Digital Network (ISDN) and the analogue Public Switched Telephone Network (PSTN) [Halsall, 1998].

As messaging systems continue to advance and global standards are established the problem of being able to communicate across differing systems will be reduced. However the ability to translate messages so that they may be passed over different systems and onto different devices continues to be a problem.

2.2.3 Redirection problem and location awareness

As the devices that people are able to communicate through continues to increase, so does the problem of being able to determine which device should be employed to communicate with them the - “redirection problem”.

Should a telephone system be able to determine that a person has their cellular phone turned off and therefore forward the caller through to their pager or

electronic mail system? As society becomes faster paced the answer to this question becomes yes for an increasing number of people. More and more users will require their messaging systems to determine which of their communications devices, and which of their intended recipient's devices, is the most appropriate delivery channel for any given message. This determination should be based on proximity to the recipient. This would require knowledge of the recipient's location, also known as location awareness. This means that the system knows the geographical location of the user. For example a brief and urgent email message might be most appropriately delivered as a text message on the recipient's cellular phone.

Any system that addresses the redirection problem must also face the problems of translation and communication, because most redirected messages must be translated before they can be carried on a different messaging system, and then communicated to the intended recipient.

Current research and development in messaging systems is focused on solving additional problems beyond the fundamentals of communication, translation and redirection. For example, there is a large body of published literature on a variety of "security problems" in messaging systems, such as the prevention of eavesdropping, and (for location-aware devices) the non-disclosure of a user's current geographical location.

While security issues are discussed in more detail in Section 6 below, this paper's primary focus is on the "persona problem". Our literature search uncovered a small amount of relevant material not cited by Li see Section 3.2. Defining what is meant by "persona" begins the development of the persona concept.

2.2.4 The Persona

From the Greek word meaning "actor's mask", the term persona refers to the "face" or a role a person will adopt in given situations [Geist, 1998]. Each person may have one or many of these personae that they may adopt over

their lifetime or in the course of a day. In everyday life people are familiar with this concept but may not be consciously aware of its use.

The concept of a persona is well developed in the psychoanalytic theories of Sigmund Freud and his successors, notably C.G. Jung [Geist, 1998]. Somewhat surprisingly, the computing field has taken little notice of the persona concept, even in the field of computing research known as "human-computer interaction" (HCI) design. The central issue in HCI design is to find ways in which designers could make a user's interaction with computers easier and friendlier. Artificially intelligent computer programs are sometimes given persona. Examples of these are Microsoft's Peedy and similar software agents that may be programmed to interact with the user [Ball, 1997].

2.2.5 Persona problem

The persona problem relates to a messaging system being able to identify and incorporate a user's predefined differing identities and process information accordingly. This raises the issues of privacy and anonymity (see Section 6). One area of this problem that this paper examines in more detail is the concept of persona identification. This is the incorporation of the user's personae into a fifth generation messaging system. This concept is explored in Section 3.2.3.

Before doing so a brief review of the history of messaging systems to date is presented. This history is a summarised version of that provided in Li's Masters thesis with additional references noted.

3. Messaging systems

3.1. A brief history

Sven van der Meer, Stefan Arbanowski and Dr Thomas Magedanz suggest there are four generations of messaging systems in their paper "*An approach for a 4th Generation Messaging System*". The first and second generations of messaging systems are described as asynchronous communication services. In other words, users do not directly communicate with each other. Instead the calling party sends information as a message. This is stored in the system until the recipient accesses it at some later time [Van der Meer, 1999].

In the first generation of messaging systems a sender would send a message to the recipient via one of several devices such as facsimile, e-mail or voice-mail. The recipient may then check and retrieve these messages from that particular device.

Figure 1 depicts the method of message transfer in a 1st generation system. A sender is able to send to the recipient Bob, a message on any one of the listed devices. Bob can then check each of the listed devices for incoming messages.

Checking numerous devices for messages created frustration and was a time consuming practice for users. So solutions to this problem were sought.

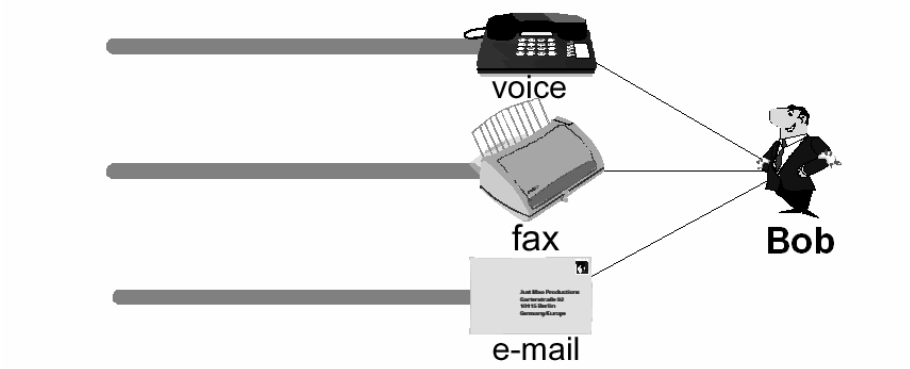

Figure 1 1st generation messaging system [Van der Meer, 1999]

First generation messaging systems provide a solution to the communication problem identified in Section 2.2.1 of this paper. The call-forwarding feature of the Public Switched Telephone Network (PSTN) is a partial solution to the redirection problem, however its redirection is limited to other devices on the PSTN network.

Integrated messaging systems combine the several mailboxes of the different devices into one universal inbox and were introduced in the second generation of messaging systems. These systems provide a solution to the frustration some users were experiencing with multiple messaging devices. E-mail provided a convenient technological infrastructure for integrated messaging, as

email is able to integrate a variety of multimedia objects such as Multipurpose Internet Mail Extension (MIME) attachments.

In a typical integrated messaging system, voice and fax messages are sent as attachments to e-mail messages, as shown in Figure 2.

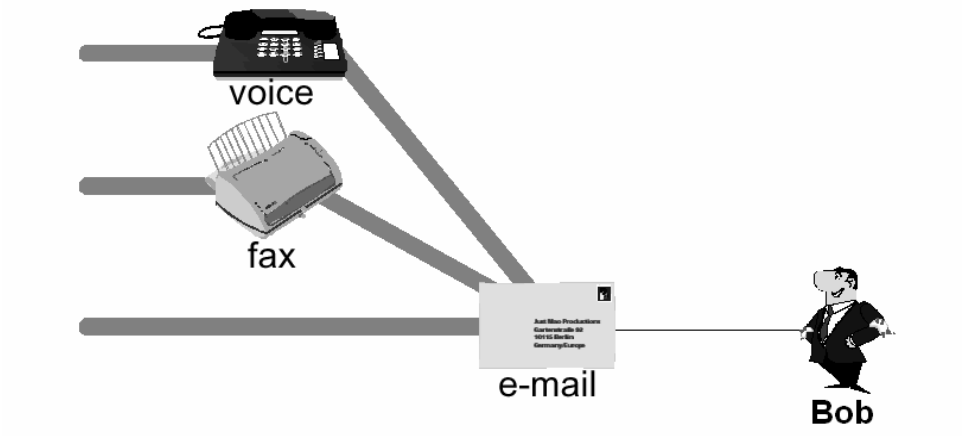

Figure 2 2nd generation messaging system [Van der Meer, 1999]

Note that all incoming messages are directed into a single inbox for the user. Bob is able to receive all of his voice, fax and email messages by checking his email. If Bob is happy to use email for all of his incoming messages, then he no longer has translation and redirection problems with his incoming voicemail and faxes. However Bob still has translation and redirection problems in an integrated messaging system if he wishes to pick up his messages by any other medium.

These problems are largely overcome by the third-generation systems known as “Unified Messaging” systems.

Unified Messaging (UM) is a service that combines voicemail and faxes from a voice environment with email from an IP (data) environment. Unified messaging allows users to manage, access, and store voicemail and faxes like email, and to access email the same way they access voicemail [Anonymous, 2002].

In Figure 3 these third generation systems are shown to provide access to the centralised stored and managed information resources for all of the major

communication services, including touch-tone phones, fax polling and e-mail retrieval [Van der Meer, 1999].

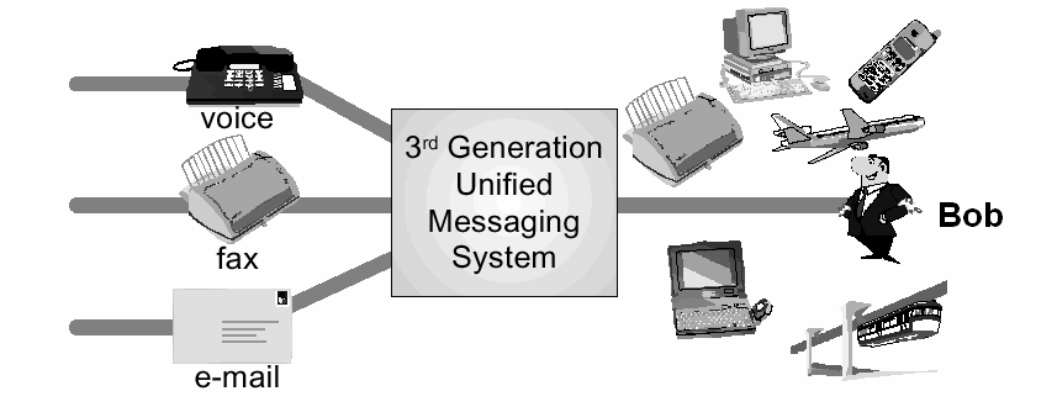

Figure 3 3rd generation messaging system [Van der Meer, 1999]

Such systems adopt methods such as Text-To-Speech (TTS) techniques to read fax or an e-mail to a user. This conversion method was an advance towards solving the translation problem defined in Section 2.2.2 of this paper.

Van der Meer et al. suggest a fourth-generation system must support the user by a seamless integration of new network access technologies, new terminal equipment and new multimedia applications. This must include distributed processing, intelligent mobile agents and location aware applications. These systems must also account for the fact that the main interest of users is not ubiquitous access to their messages but control of their reachability [Van der Meer, 1999].

Figure 4 shows the concept of a fourth generation messaging system. Any type of media may be used to send a message, which is then translated into the required format and forwarded to the device designated by the user.

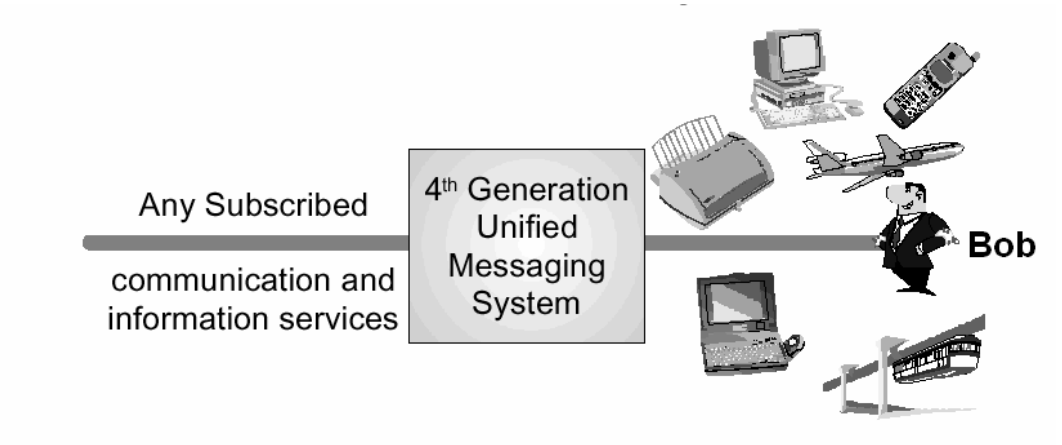

Figure 4 4th generation messaging system [Van der Meer, 1999]

This fourth generation system model provides a solution to the communication problem defined in Section 2.2.1 of this paper. By being able to invoke the appropriate conversion technology to deliver received messages this system provides a partial solution to the "redirection problem" by allowing users to define where they wish their messages forwarded. Yet as noted by Li in her thesis the fourth generation model does not mention several key areas including:

- Sequential redirection, which refers to the rerouting of a message to the appropriate device and using several devices over time to see the message successfully delivered.
- Mobile person's privacy protection, or privacy and anonymity in this paper (see Sections 6.1 and 6.1.3).
- Redirection according to the information's priority, the ability of a system to evaluate messages to let users have their incoming communications prioritised and filtered according to their preferences, then have the message sent according to the information's priority.
- The "persona problem" [Li, 2001].

3.2. 5th generation messaging systems

In her thesis "*A fifth generation messaging system*" Li examines the feasibility and structures of a proposed model for a fifth generation messaging system. This system would integrate the voice and Internet networks on an IP-based

architecture. It would also be able to integrate different services from heterogeneous networks. Included in the system design are conversational, messaging and retrieval services.

3.2.1 Fifth generation system architecture

The architecture of a fifth generation system is designed with three parts to its architecture, a client, a server and a network. A server provides the service and the service communicates through a network to a client's device [Li, 2001]. The architecture of this system would allow for integration of legacy communication systems and the scalability to integrate it with future communication systems.

3.2.2 Fifth generation system catalogues

The first area of the system examined is the inclusion of the message delivery catalogue. This is concerned with the exchanging of messages between the sender and recipient. It is not concerned with the actual processing of messages. The message delivery catalogue characterises the manner in which the following features are adopted:

- Initiating ability allowing both senders and recipients to initiate a call.
- Distributing facilities whereby the system sets up a separate call for each recipient.
- An alerting feature to help trace a message's path.
- Certifying feature to confirm delivery of a message to a sender should they request it.
- Redirection (rerouting) of messages to allow faster retrieval of messages and solve the redirection problem.

This redirection requires the knowledge of the user's current location (location awareness) and device proximity. Li discusses the Mobile Person Architecture (MPA) proposed by Maniatis et al [Maniatis, 1999] to help achieve these goals. The MPA focuses on providing ubiquitous reachability and maintaining location privacy. A personal proxy is described in the framework, which acts as a tracking agent maintaining a list of devices or applications that

the user is currently contactable through. It also acts as a dispatcher, directing communications and using application drivers to convert the messages into a format the user is able to see immediately [Maniatis, 1999]. An alternative model that was not examined in Li's thesis is described in Section 3.2.4.

The second area is the message processing catalogue. This defines the properties that characterise message translating, storing, ordering and filtering. These properties are defined in the following features:

- Translating of message formats including multiple times during one delivery period.
- Ordering or prioritising of messages to determine delivery importance.
- Filtering ability, allowing the system to determine whether it wishes to accept the message or not.

One area that is briefly discussed and informally examined in the thesis that is relevant to the message processing catalogue is the inclusion of the persona concept or a step towards a solution of the persona problem as proposed by Li. The incorporation of this idea would largely affect the processing of messages in the system. Li mentions that the inclusion of such a concept in a fifth generation messaging system could provide some additional functionality to a user. In this paper this idea is discussed as persona identification and discussed in more detail in Section 3.2.3.

Thirdly the message security catalogue of the system, which addresses:

- Non-intercepting, ensuring that the system does not allow anyone but the intended recipient(s) of the message to receive and interpret it.
- Non-repudiation, where neither the sender nor the receiver may deny that they have sent or received the message.
- Non-replaying, where the system protects messages for replay attacks. A traditional replay attack in the cryptography sense is an attack in which a valid data transmission is maliciously or fraudulently repeated, either by the originator or by an adversary who intercepts the data and retransmits it [Pennington, 2001].

- Non-tracing, ensuring the system is able to protect the sender and receiver's location privacy (see Section 6.1.3.1).

Finally the message failure catalogue addresses:

- Failure range, which determines what range of delivery is classed as successful. Typical ranges of delivery are "any recipients, any device" and "all recipients, all devices".
- Failure level, which defines a message's success based on either
  - Delivery level (successful delivery)
  - Processing level (successful delivery and correct response received) or
  - Security level (successful delivery, correct response received and a satisfied security request).
- Failure handling of messages, where the system decides what procedure to undertake should a delivery failure occur.

Having discussed systems to date and Li's proposed model, this paper now examines "persona identification". This concept is a derivative of Li's "persona problem" clarified and redefined in Section 2.2.5.

3.2.3 Persona identification

The persona identification concept is the system's ability to identify a user's persona or personae. Information relating to these personae can then be processed accordingly. The proliferate use of tag names in Instant messaging systems suggest that this concept of persona identification or management should be incorporated as a feature in a fifth generation model. The benefits of such a feature in the system are discussed in Section 5.

Current systems store information about a user's profile, for example personal preferences, name, login, password etc. A fifth generation system would be able to take this concept one step further, extending a central concept in a

system patented by William Bunney [Bunney, 1999]. This patent was not examined in Li's Masters thesis.

Bunney describes an Internet based system that uses a server and numerous user terminals. It includes a Profile Manager that maintains a database of user profiles. Each user has at least one user profile that contains commonplace information about the user but also sensitive information that must be kept strictly confidential. In addition to this compulsory profile a user may have one or more additional profiles associated with them. Each of these profiles is assigned an individual address each representing a different personality for that user. Each profile may be displayed as invisible, busy, away or available for communication [Bunney, 1999].

By extending Bunney's system to enable storage and identification of information regarding user's personae, a fifth generation messaging system would be able to determine through a set of predefined rules which persona was in operation at what time and conduct message transfer accordingly. For example Bob may have defined two personae in the system, a Personal persona and a Professional persona. During his work hours all messages that are identified by the system as professional are directed to his work phone or email depending on his location and device activation. All messages that are identified as personal but not family orientated the system will direct to his personal email account. Messages from direct family members are identified as exceptions and depending on the priority placed on them are directed to his mobile phone or work email.

In our search of the literature and the practice of computing, only one currently active system has been found that allows its human users to adopt various personae. Instant messaging or IM-ing is a fast growing method of communication that has grown in popularity because of its instantaneous nature, bypassing the annoying lag time inherent in sending and receiving e-mail [LaGesse, 2001]. Through its prosaic "buddy list", a continuously updated window that shows who among your family, friends and colleagues are online and available, Instant messaging provides you the benefits of connecting you to your inner circle in a way that phones and e-mail can't [Cherry, 2002].

A user of a typical instant messaging system may adopt a tag name to express a different, fictional, or exaggerated personality or persona of that user. Users may thus adopt different skins or personalities to help them conduct their affairs, and they may explore different areas of their personality that they otherwise may not [Zeise, 2002].

For example Bob may have a professional tag “Bob Work” to let other buddies on his chat line know he is in professional persona mode. In his personal persona Bob may adopt a “Bob Home” tag.

Most of the large instant messaging systems require users to register and use a login name to access the system – this login is generally a user’s tag name identifying that particular persona. The widespread use of this tag functionality suggests that users would find it beneficial if a feature of a similar nature (persona identification) is incorporated into a fifth generation messaging system. Li did not discuss these aspects of instant messaging in her thesis.

To help develop this idea of persona identification this paper proposes a graphical user interface design and implementation in Sections 4 and 5. This paper now examines a system that would be beneficial to a fifth generation messaging system that was not examined in Li’s thesis.

3.2.4 Presence Awareness

As mentioned in Section 3.2.2 Li’s system discusses the Mobile People Architecture [Maniatis, 1999] to provide location awareness of users. A feasible alternative or addition to these methods would be to implement a presence awareness model into the system.

Presence awareness refers to the ability of an intelligent agent (computer or device) to determine an object's location within a given geographical area. By making the distributed information more context sensitive, this location-specific data optimises the execution of business processes [DiamondCluster, 2001].

Early systems for presence awareness used video cameras and gathering information from a user's login to determine user location. These approaches did not always provide presence information about a user per se, but rather about a person at a particular location [Handel, 2001].

DiamondCluster examines this awareness from a different angle in their white paper "*Presence Awareness: Optimizing the Marketplace*". In this paper DiamondCluster offers an implementable and currently used method of location detection that would provide a form of presence awareness. They discuss radio frequency identification systems (RFID), which use radio waves to transfer information between base stations.

These RFID systems integrate four application group systems, which are:

- Identification systems, which are in common use today such as SmartCards, access control cards and inventory tags used in retail stores.
- Positioning systems that are able to locate a resource in a given geographical area.
- Data capture systems that use hand held terminals to capture data that is transmitted to a host information system.
- Networked systems, which are generally fixed position readers, deployed in a given site and connected directly to a networked information management system.

RFID systems are currently in use by companies such as Federal Express, Chevrolet Creative Services, and the Ford Motor Company in the United States.

Developing these concepts Christein et al. propose a presence awareness model in their paper "*A General Purpose Model for Presence Awareness*". This model encompasses the ability of a system to locate a user in a given geographical area and determine device usability. Their model encompasses four types of entities: location, presentity, watcher and vicinity [Christein, 2002].

3.2.4.1. Location

Location is a virtual or real place where someone or something is located at or is *present*. These locations may be specified by URLs, IP addresses, on-line chat rooms, postal addresses or Global Positioning System (GPS) co-ordinates to name a few.

3.2.4.2. Presentity

A presentity is an entity that is present at a location. This does not have to be human. It may also be a running program, a robot or a user agent. Each presentity is identified by a unique identifier and has relevant information regarding it stored within the system.

3.2.4.3. Watcher

A watcher is an entity interested in presence information. This entity may also take the role of a presentity at the same time and vice versa. A watcher may obtain the required information in a variety of ways including taking a snap shot of current presence information or may poll the presence information at regular intervals.

3.2.4.4. Vicinity

A vicinity is a set of locations which are adjacent in terms of awareness. This means that any two presentities, which occupy any two locations within a vicinity will be aware of each other. These vicinities may be either static or dynamic. Static vicinities are specified by a fixed set of locations. Dynamic vicinities on the other hand may shrink and grow.

This presence awareness model is described in two manners, either presentity-based or vicinity-based. Presentity-based presence awareness allows the watcher to recognise if a presentity is currently present or not and if so at which location. Vicinity-based presence awareness provides information about which presentities are within a certain vicinity as well as their exact locations.

The prototype of Christein's model has a client/server architecture making it highly compatible with the structure discussed by Li. The current prototype

uses the Java API although compatible alternatives such as the SIP (Session Initiation Protocol) have been suggested. This implementation also relies heavily upon synchronous groupware or computer-supported cooperative work systems (CSCW). CSCW is programming that enables real-time collaboration among geographically distributed work group members [Grudin, 1994].

An important security issue raised by presence awareness systems is privacy. Businesses and users of today will not integrate or use a system that does not provide this. This issue is discussed in Section 6.1.

3.3. Applying Christein's model to Li's system

Christein's presence awareness model accommodates not only human but also mechanical and artificial intelligence interaction with the system. Such a model could provide a stronger structure for location awareness for a fifth generation messaging system. By adopting this model Li's fifth generation system could find itself in demand in today's market.

This fifth generation messaging system is built on the previously defined fourth generation system. It attempts to fully solve the three problems mentioned earlier in this paper and incorporate the persona identification concept.

Having examined alternative methods of implementing persona identification and location awareness, development of an electronic mail system that recognises three personae is now presented.

Firstly the design models for such a system are examined. Then the user interface design guidelines on which the proposed interface has been designed are discussed before examining an existing e-mail interface. In the Future Works area of her thesis Li discusses the need for a *user interface*. In this paper an area of this topic is examined by presenting a possible graphical user interface for an e-mail system that a fifth generation could incorporate. The

complete user interface design for a fifth generation system is an area of future work.

4. Designing an electronic mail interface

4.1. Design decisions

Defining the boundaries of a user's personae is one of the hurdles in developing a messaging system that successfully addresses the person problem. Bunney's patent and Li's thesis are silent on this "persona boundary" issue, so this section is devoted to a careful discussion of this issue.

The starting point is a simple example in which Bob has identified two personae that he wishes to work with, his Professional and his Personal personae. His Professional persona relates to his affairs during work hours and his Personal persona relates to his affairs outside of work time. The persona boundary issue arises when these two personae overlap. For example Bob's friend Joe may be a work colleague as well as a tennis partner. Is Joe classified with Bob's Professional or his Personal persona?

In designing a system that will incorporate the persona identification concept, design guidelines to make decisions about these kinds of classifications must be established. Either the design may allow overlap in these personae thereby adopting an overlapping model or not allow overlap giving clear distinction on a persona's limit. This paper briefly examines both ideas and concludes with the design decisions made for the user interface developed here.

4.2. Overlapping model

In an overlapping model persona entities would not have clearly defined limits. A persona may find through its definition that it requires information from another persona or may require the use of some functionality provided by different persona. This approach allows for interaction of persona. A suggested theoretical framework for implementation of overlapping persona is to adopt the "fuzzy set logic" approach [Zimmermann, 1992].

Figure 5 depicts an over-lapping design for the persona model, in this case adopting three defined persona. A super type (Archetype) encompasses two child types – Professional and Personal. The Archetype, Professional, Personal entities each contain sensitive information about the user and particular persona. Archetype holds information that is found in both the Personal and Professional entities. With this model aspects of each entity may overlap. An implementation example of this is Bob's friend Joe being associated with his Personal and Professional persona rather than one or the other.

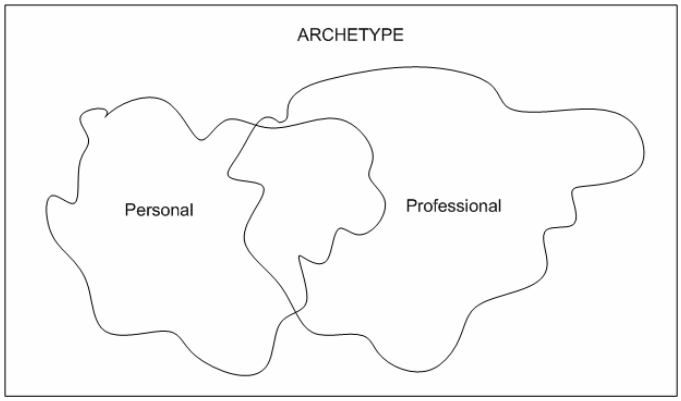

Figure 5 An overlapping persona model

This approach becomes problematic when decisions about message delivery to the individual persona must be made. An overlapping model might be difficult to implement effectively and could cause inefficiency within a system, especially should system users decide more persona are necessary. Because solutions to these difficulties have not been found, further discussion of the overlapping model is beyond the scope of this paper.

4.3. Non-overlapping model

The non-overlapping system model is now examined. As today's technologies advance a widely accepted method of design is the Object-Oriented approach. With this approach objects relevant to the system are described and determined along with their relevant attributes. The user and administrator of the system could predefine each persona as an object and each associated entity (such as Joe) is classed to its relevant persona.

Figure 6 depicts a non-overlapping model, in an object-orientated implementation. In this model the super type Archetype is a shell holding minimal information relevant to both children entities – Personal and Professional. This information is inherited by the Personal and Professional persona but all associated entities are associated with only one of the three entities. No overlapping is allowed.

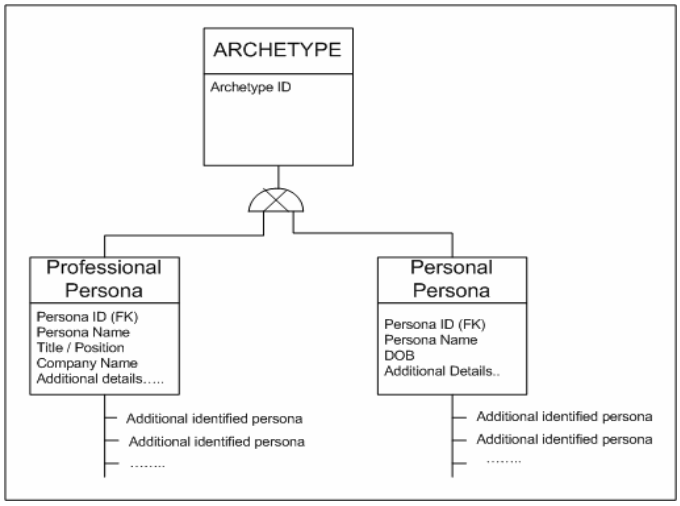

Figure 6 A non-overlapping persona model

With these confinements preventing entity overlap comes the problem of defining a persona within a persona. Bob may find his Professional persona too broad and wish to define another persona such as an Office Professional persona that deals with all matters pertaining to his time in the office where as his Travel Professional persona deals with matters pertaining to his time elsewhere. From here these persona could be redefined, re-established and split again as the scope of each persona increases and becomes too broad once more.

This paper adopts a non-overlapping persona model that allows additional sub-persona to be created from the predefined second hierarchical level persona. A structure for these sub-personae should be carefully designed to prevent problems with persona management. This design structure is an area of future work in a fifth generation system.

This paper now examines guidelines for the design of an e-mail user interface.

4.4. User interface design guidelines

In today's computing environment three main, recognised interfaces are used. These are the Command Line Interface (CLI) as adopted by the Unix operating systems such as Linux, a menu interface often adopted by large corporations such as retail outlets and the Graphical User Interface (GUI) made famous by Microsoft Windows. The GUI interface provides drag and drop operations on the objects defined by the operating system or application program.

The User Experience, or how the user experiences the end product, is the key to acceptance. That is where User Interface Design enters the design process. While product engineers focus on the technology, usability specialists focus on the user interface [Galitz, 1997].

With usability being a major issue with a system, users often prefer an environment they are familiar with. A majority of the populace is familiar with the GUI design. For this reason the interface designed in this paper adopts a GUI style format.

Microsoft Consulting Services give eight high-level design principles that should be considered when designing a user interface:

- Consistency
- Clarity
- Feedback
- Aesthetics
- Directness
- Forgiveness
- User Control and
- Human strengths and limitations.

A well-designed, well-presented, consistent user interface will increase the extent to which users consider the "system" to be easy to use, and it is more likely to generate a feeling of confidence in their capacity to retain mastery,

enjoyment of using the system and a competence in task performance [Microsoft, 1993]. Additional areas that should be taken into consideration include:

- Efficiency
- Predictability and
- Simplicity

Without these key areas users would find the interface irritating and cumbersome to use and thus disengage from it [Galitz, 1997]. With these points in mind a design of an e-mail user interface that could be used in a fifth generation messaging system is developed.

5. Developing an electronic mail interface

5.1. Microsoft Outlook

One particular e-mail interface that is well known and often used in a business environment is Microsoft Outlook 2000. This paper examines the design of the Microsoft Outlook 2000 interface with respect to the guidelines presented above. Figure 7 is the Microsoft Outlook 2000 interface that will be used as a design base for the proposed e-mail interface. The numbering within the figure is used as references in the following section.

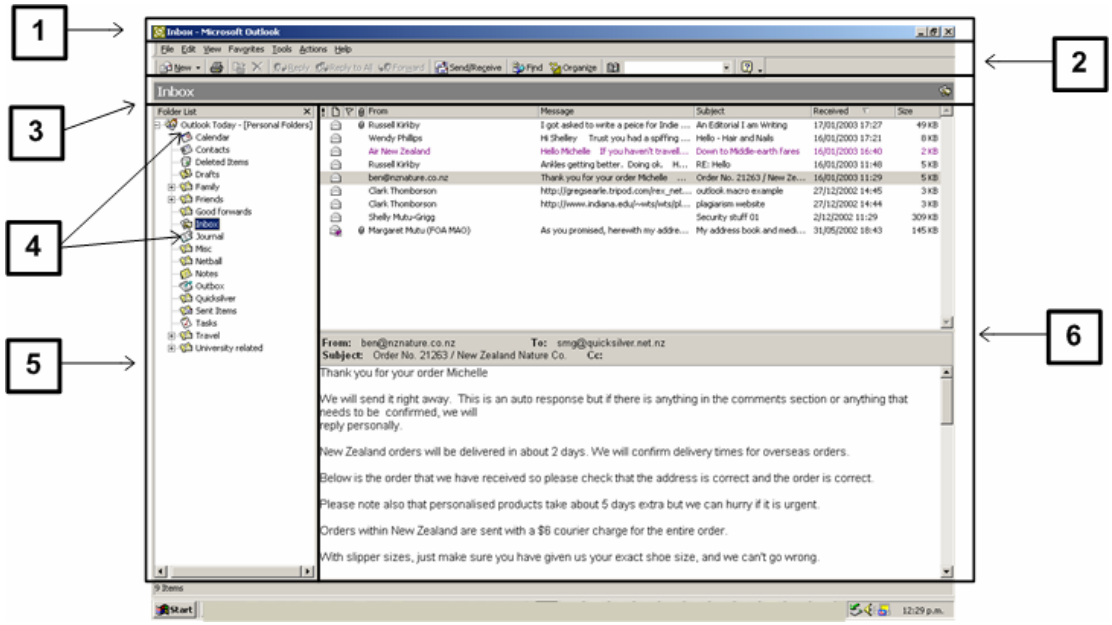

Figure 7 Microsoft Outlook 2000 interface

Microsoft Outlook 2000 is an application produced and supported by the Microsoft Corporation. It is a client designed front-end application that is designed to work in conjunction with a server side program such as Exchange or a Web based Internet (or similar) mailing system. It is a convenient application with a "user-friendly" interface that aids users handling email. Microsoft Outlook 2000 contains many additional features including Calendar and Journal features that are not examined in this paper.

In this version of Microsoft Outlook the interface adopted is based largely upon the Microsoft application interfaces found in Microsoft Word or Microsoft Excel.

The interface follows top to bottom layout. By providing meaningful contrast between screen elements and the simple and effective use of colour [Galitz, 1997] Outlook 2000 provides an aesthetically pleasing environment for users to work in. This follows the Aesthetics design guideline presented by Microsoft Consulting Services.

Area 1 in Figure 7 is a blue panel indicating to the user the name of the application that they currently have active. Below this is a selection of menu toolbars (number 2 in Figure 7) that a user may interact with to draft, send and manipulate both e-mail and the application. As with other Microsoft applications these menus can be customised to suit a user's preferences. The user is able to decide which menus it wishes to have in its current view and may remove buttons from these menus should they choose to. By having this manipulation available to the user the interface is providing the design principle of User Control. In addition to this, the similarity this interface has with other Microsoft applications follows the Consistency design principle suggested by both Microsoft and Galitz.

The panel below the menu bars (number 3 in Figure 7) is an indicator panel telling the user which part of the application they are currently interacting with. As a user manoeuvres through the application this panel updates as necessary. This technique follows the Feedback design principle that helps guide the user

in their navigation. By depicting a clear picture and providing tool tips that appear as a user moves their mouse over a button on these menu bars the interface incorporates the design principle of Clarity.

Below this panel and to the left, the hierarchical filing system that Microsoft Outlook adopts is seen (number 5 in Figure 7). It allows a user to organise e-mail into either predefined or personalised folders in the filing system. The provision of expansion or collapsing options in the filing interface makes efficient use of the interface's space. By employing this design the interface incorporates the Efficiency design principle. Number 4 in Figure 7 is the area where the Calendar and Journal functions are also accessed.

Within the application are programmed features to ensure Directness, Forgiveness and to account for Human Strengths and Weaknesses. An example of these is the method of double-checking a user's action when a user attempts to exit the system with outgoing emails that have not yet been sent. In such a case a user must confirm via a pop-up window (incorporating the Directness design principle) that they wish to exit the application while the messages remain unsent or return to the application and ensure the outgoing messages are sent. By requesting a user examine their actions the application is catering for the Human Strengths and Weakness design principle. In completing this action the system may prevent an accidental deletion of an important document incorporating the Forgiveness design principle. Forgiveness ensures that there is as little delay as possible with sending e-mail messages, even if a "Human Weakness" invokes a premature program exit.

In Figure 7 number 6 shows one customised view a user may choose to view their e-mail with. This view shows all non-filed e-mail in the user's inbox. By selecting one email the user may view its contents. Again this view may be changed to the user's personal preference.
Having examined the Microsoft Outlook interface the design proposed by this author is now examined.

5.2. Proposed persona identification user interface design

To allow for usability a system interface should be predictable and straightforward to interact with to obtain the desired results. By adopting a well-known interface design base (Microsoft Outlook 2000) the Predictability and Simplicity aspects of design mentioned above are adhered to.

The proposed design is able to identify and process messages for one parent persona – Archetype and two children personae - a Personal and a Professional persona. Once this design has been presented a method of implementation with the Microsoft Outlook 2000 system is discussed.

Figure 8 shows one possible view of an interface with the persona identification concept implemented. It shows a maximised view with the two inboxes and message previews for the selected emails.

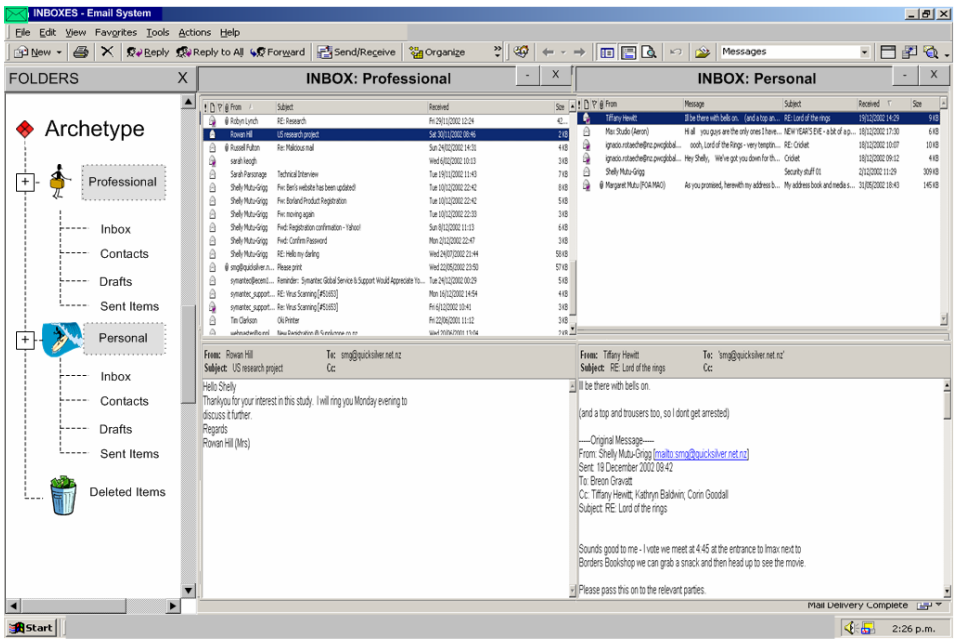

Figure 8 Interface view: Dual persona inboxes with preview

The structure of the original interface remains unchanged, but two inboxes replace the previous single inbox. The additional functions such as the Calendar and Journal have been removed to illustrate the persona implementation concept clearly.

This graphical user interface displays inboxes for two personae, one professional, and one personal. A user is able at a glance to see both their personal and professional email. The parent Archetype is used for e-mail that the system is unable to identify its associated persona. A user is able to occasionally check this inbox and determine which persona these e-mail should be associated with.

Figure 9 shows an example of how a user would be able to hide their Personal persona. By having this feature enabled a user is able to disregard email that is personal during their professional hours and disregard their professional email during personal hours. For example if Bob is at work and in his Professional persona he is able to hide his Personal inbox until an appropriate time when he may wish to check his Personal persona messages.

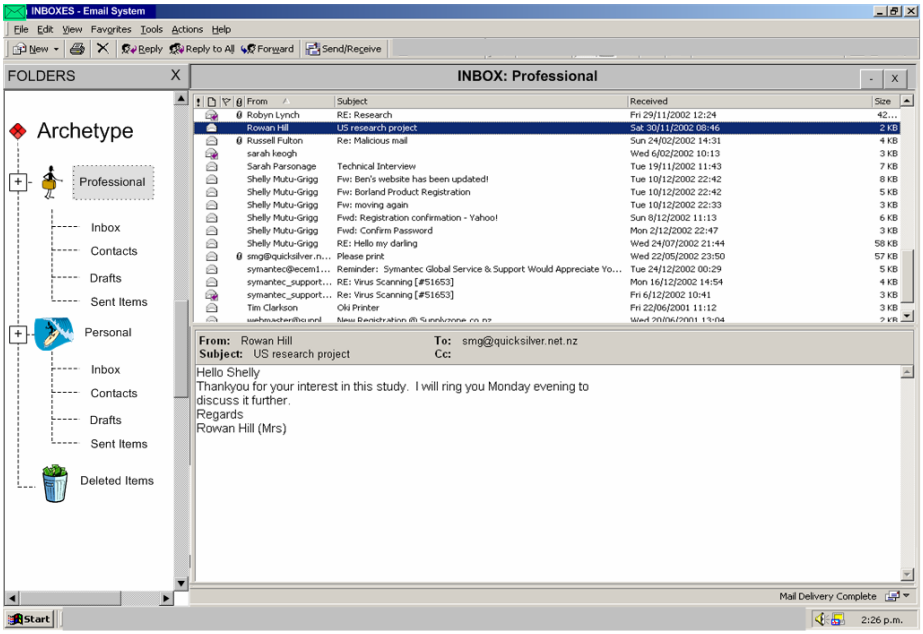

Figure 9 Interface view: Professional Persona Inbox with preview

From a user interface point of view implementation of the persona identification concept is relatively straightforward. It is simply manipulating the current interface to provide the required functionality such as the required number of inboxes in this implementation.

So it is clear on an interface level that the persona identification concept is possible to be incorporated into a fifth generation messaging system. On a

practical level many work environments discourage employees from using their working time to conduct personal affairs such as email or telephone calls to friends or family. The use of such a mailing system could help companies be more productive by helping staff separate professional and personal email.

A possible method that could implement the persona identification concept on a deeper application level is now examined. Then a current feature in Microsoft Outlook 2002 that could aid in the implementation of the persona identification concept is looked at.

5.3. Persona identification implementation with Microsoft Outlook

In relation to the Microsoft Outlook application a possible implementation of the persona identification feature would be to have a persona "filter" that would need to be run in conjunction with Microsoft Outlook. This filter would be based on a variety of rules set out by the designers and additional rules added by the individual. This filter must be capable of interfacing with legacy systems and it must also cater for scalability that is for the ability to grow with implementations of new systems.

A method of creating an e-mail filter that is currently available in Microsoft Outlook 2000 is now examined. In Figure 10 it is possible to see how a user is able to access the Rules Wizard function available in Microsoft Outlook 2000.

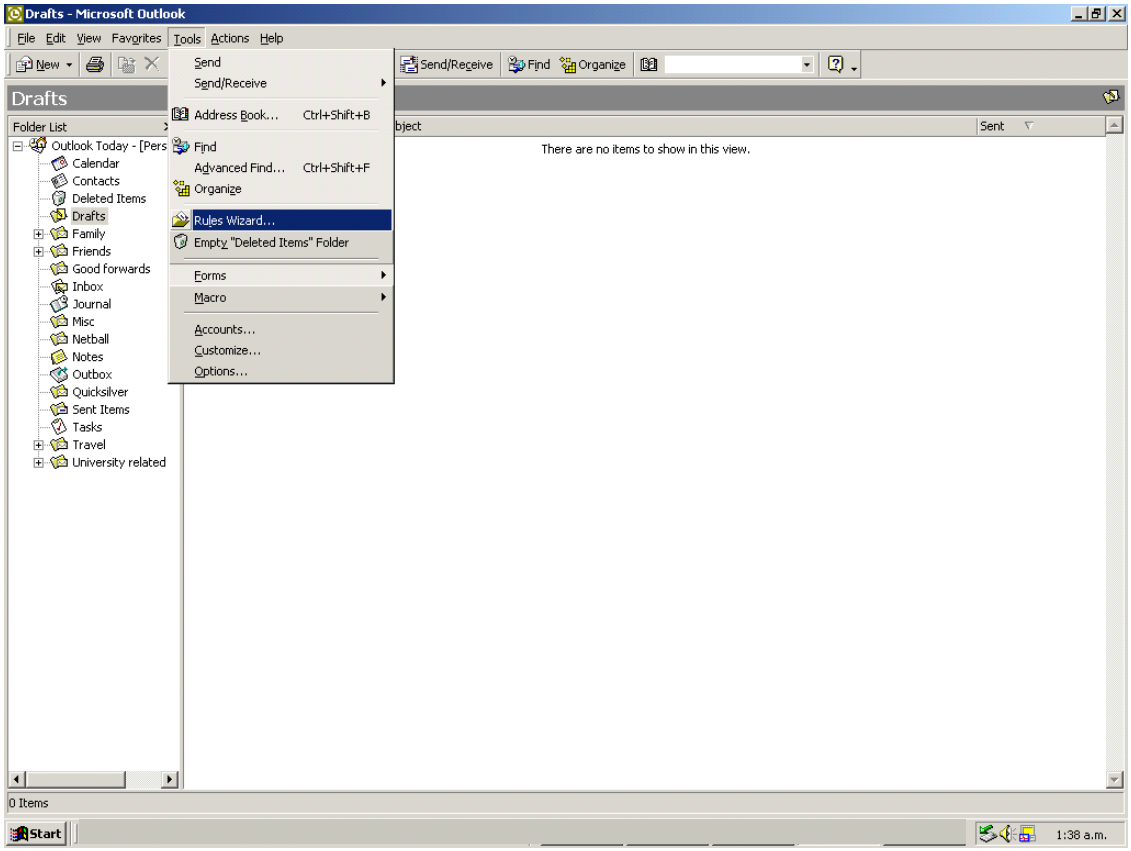

Figure 10 Rules Wizard access in Microsoft Outlook 2000

This wizard walks a user through the creation of customised e-mail filter that a user may create. A user is able to select at what point the filter becomes active, for example either upon email receipt or transmission. They are then able to select from a series of rules that identifies the need for activation of the customised filter. For example if the e-mail header contains an identified key word or a particular account is being sent to, then the filter will be applied to the e-mail by the system. Figure 11 depicts some of the choices of rules a user may decide to use in the filter's activation.

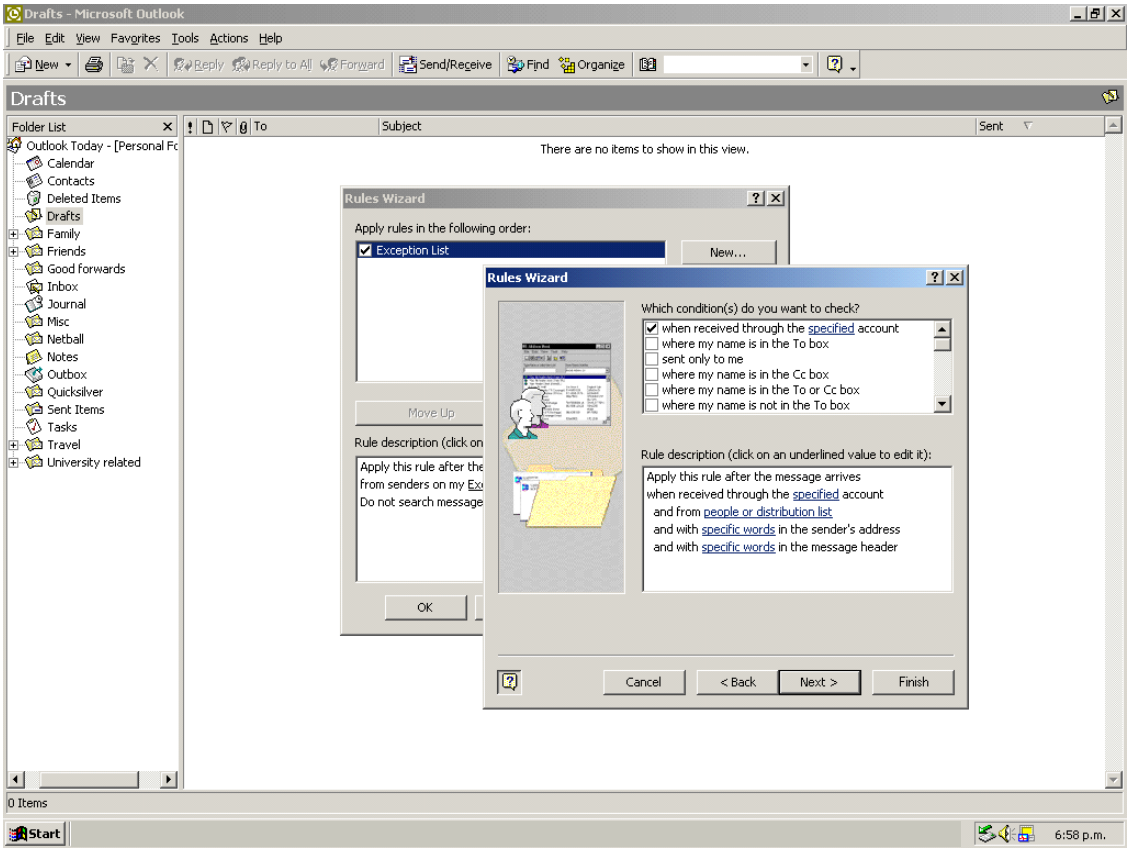

Figure 11 Rule selection in Rules Wizard in Microsoft Outlook 2000

However the limitations imposed by the predefined rules available in Microsoft Outlook 2000 prevent implementing the persona identification functionality properly. For example a filter could be based on a persona's contacts list. Any contact that is defined in each persona will have all messages from that contact directed to the associated persona. With this rule comes the distinction that a contact may not appear in more than one persona adhering to the non-overlapping design model described in Section 4.3. In the Microsoft Outlook 2000 Rules Wizard a user is able to identify a distribution list. Such a feature could be extended to allow for a persona's contact list.

There is also a macro construction available in Microsoft Outlook 2000; however the additional security risks this option presents has stopped the author of this paper from proceeding with this line of investigation.

Due to the restrictions of copyright and industry protections, design, programming code and construction of the Microsoft Outlook application cannot

be examined. However current functionality is examined to suggest a program implementation.

In Microsoft Outlook 2002 there is functionality provided allowing an administrator to create a "profile" or profiles. These profiles are Outlook's way of remembering e-mail accounts, data files, preferences and option settings for individual users. They allow different users to use the same machine but retain user's personally defined customisations of Microsoft Outlook [Barich, 2001]. However the same user cannot use these profiles concurrently. A user must log in and log out of a particular profile. This functionality could be extended so each profile could be identified as a particular persona and if information regarding these profiles or persona were able to be processed concurrently then the implementation of the persona identification concept would be possible.

To have this concept implemented with Microsoft Outlook discussion and design would have to be undertaken in conjunction and with the permission of the Microsoft Corporation.

5.4. Filter and alternative persona identification implementation

Another method of implementation could be to base the implementation of the persona identification concept on currently available filters or proposed methods. Filters can be built based on a variety of information. The filter this paper examines relies on addressing information contained in a message.

5.4.1 A filter that relies on addressing information

One scheme that is designed to combat spam (unsolicited commercial mail) which could be adapted to provide a persona filter is that proposed by Scott Fahlmann in his paper "*Selling interrupt rights: A way to control unwanted email and telephone calls*" [Fahlmann, 2002]. In his paper Fahlmann presents a scheme that provides a way of billing users that wish to contact a person. His proposed solution has three parts. The first part is:

1. Each account has an accept list that is maintained by the user, which will allow anyone on that list to contact the user without interference.

This method of identification uses the sender's information to authorise the system to accept the incoming message without interference. If this method of accepts list was modified to incorporate an accept list for each persona, this would help implement the persona identification concept into a fifth generation messaging system. The second and third parts of Fahlmann's model are:

2. The user may create interrupt tokens (for single use only) and provide them to people and companies that have a legitimate need to contact the user in the future.
3. Uninvited callers or mail senders must make a binding offer (undertake an agreement to pay the required fee) to pay an interrupt fee to the recipient.

A sender in the system must identify whom they wish to contact. Once this decision is made if they are not on a user's accept list then they must obtain a token for that user. The system will generate this token using the recipient information in the message.

This charge may be waived if the contact is valid and unobtrusive. In this model uninvited callers or mail senders would go through a process to obtain an interrupt token either via an automated telephone system or on a secure link on the Internet, which they may then use to contact the desired user.

By incorporating this part of Fahlmann's model a fifth generation messaging system would be taking a step towards providing the *Billing Integration* feature mentioned in Li's Future Works section. Fahlmann's scheme should be examined as a future work to accommodate this feature.

Another filter that should be examined, as future work for this paper is that described by Paul Graham in his paper *Better Bayesian Filtering* [Graham, 2003].

5.4.2 Methods that rely on addressing information

A method that does not employ filtering but uses addressing information of a message is that of Dr John Ioannidis of AT&T Labs, USA [Ioannidis, 2003]. Dr Ioannidis proposes that instead of trying to prevent spam by filtering, one should stop it before it is sent. His encapsulation policy adopts the use of so called "single-purpose addresses" or SPAs. These SPAs are generated by a program and then distributed to requested contacts. These addresses have a life span determined by the recipient [Austen, 2003].

An SPA is encoded with a security policy that describes the acceptable use of the address. These SPAs are cryptographically protected to shield them from tampering. Should this policy be abused then the address becomes invalid and messages to it are no longer received by the system [Ioannidis, 2003]. SPAs differ from Fahlmann's token scheme, as they are multi-use and do not have a time-limited existence.

Potentially if a system was processing numerous personae and each persona has a variety of e-mail addresses then Ioannidis' system could be a method of organising them. The cryptographic security features mentioned by Dr Ioannidis would be beneficial to users in a fifth generation messaging system. Ioannidis' encapsulation policy should be examined as future work to determines its implementation into a fifth generation messaging system.

Robert Hall of AT&T presents a similar method that also does not rely on filtering. Hall proposed a technique called the Email Channels system. Essentially each user's e-mail account is made accessible via a user-controlled set of channels. Each channel has a distinct structured address, which contains within it the account name and a cryptographically secure channel identifier [Hall, 1998]. Should a channel be abused i.e. be inundated with spam

mail, a user may close that channel down and notify all relevant correspondents of the change in communication channels. To help implement this and reduce complexities Hall includes a software agent, the Personal Channel Assistant (PCA), that operates like an active, enhanced address book that manages the different channels and automatically inserts the appropriate return address for each correspondent, among other functions.

The PCA prototype implementation is as an email proxy, sitting between the user's mail client and the mail server itself. All PCA interfaces use standard protocols (SMTP – Simple Mail Transfer Protocol, POP3 – Post Office Protocol, HTTP – Hypertext Transfer Protocol, FTP – File Transfer Protocol) to interact with clients and servers, so no special client software is needed to use it [Hall, 1998].

If this method was modified to allow several channels and an individual PCA per persona identified within the system, then the PCA model could conceivably be adapted to process persona information. This could provide the persona identification functionality to users. Given that Li's fifth generation system is an IP – based one, this Email Channel system would easily be able to be integrated to help provide the required functionality to users.

Having examined the possible implementations of the person identification feature some security risks raised by the persona identification concept are now examined.

6. Identified Security Risks

Security of information and privacy are prime concerns in any messaging system. Corporations and businesses of today rely on high level of security to provide them with client confidentiality and a competitive edge in the market place. Sensitive information stored within a system must be protected. As with all systems as additional functionality is added security risks are created. This paper briefly examines security issues relating to: Privacy, Integrity and Availability of Service.

6.1. Privacy Risks

Four areas of privacy identified by Li for an individual that must be addressed in a messaging system are:

- Privacy of behaviour, being able to have all aspects of behaviour kept private.
- Privacy of communication, being able to communicate with others without routine monitoring of their communications by other persons or organisations.
- Privacy of data, being able to have personal data and information private to the individual. Also known as 'data privacy' and 'information privacy'.
- Privacy of location, making it possible to have geographical location private to the individual. Also known as location anonymity discussed in Section 6.1.3.1.

Users of technology systems wish to ensure that their actions and personal and related information are kept both secure and private. Due to the 3000 percent increase in privacy lawsuits filed in the last decade in America alone businesses are increasingly bound to ensure the privacy of confidential data for staff, clients and shareholders alike [Flynn, 2001]. The key document governing a person's privacy in New Zealand is the Universal Declaration of Human Rights adopted under the Human Rights Act of New Zealand 1993. Article 12 states:

> "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." [New Zealand Parliament, 1993]

From a user's point of view, as systems today increase in their capabilities there is a fundamental tradeoff between access to data for legitimate uses, and

concerns about privacy [Godefroid, 2000]. A fifth generation system must offer its users an appropriate tradeoff.

Privacy may be provided in a variety of ways. This paper examines methods of authentication and encryption before discussing the issue of anonymity.

6.1.1 Authentication

A widely adopted method of providing communication and data privacy is that of authentication. Authentication is a process of verifying the identity of a user, device or other entity in a computer system, often as a prerequisite to allowing access to resources in a system. It is also a process used to verify that the origin of transmitted data is correctly identified, with assurance that the identity is not false. The term is also used to describe the method of establishing the validity of a claimed identity [Peltier, 2002].

For example the recipient of a message might want to verify the identity of the sender a message asking the question “What time are you expecting to arrive home?”. If the message is from a stranger the unwary recipient might reveal behaviour and location details. A fifth generation messaging system must provide an adequate level of authentication of senders. Authentication of message recipients is also important, from a privacy perspective. If a stranger is able to read a person’s messages then all four areas of their personal privacy are at risk.

There are many ways to provide Authentication in a system, Li discusses several of these options in her thesis, including:

- Password based authentication, determining authentication via a private password exclusive to the user.
- Rendezvous, the agreement of two parties on message delivery at a particular time and place.
- Symmetric cryptographic-based authentication where a claimant A proves his or her identity to a verifier B by performing a cryptogram

operation of a quantity that either both know or B supplies [Oppliger, 1996] [Li, 2001].

Authentication provides a form of communication privacy.

6.1.2 Encryption

Another method that may be used separately but is often used in conjunction with authentication is the method of encryption or secret writing. Encryption is the process of scrambling plaintext (information in its normal form) into ciphertext (information in its scrambled form) in such a way that only the recipient can recover the original information [Hughes, 1998].

Encryption may be employed in several manners including:

- Public key encryption (asymmetric key encryption), which is the method of creating key pairs, one of which is kept private, the other is made public. One key is used as a locking device, the other to open. This method also provides authentication of the user as only the owner of the private key may use it.
- Block cipher, which is an encryption algorithm that works on chunks of data at a time.
- Stream cipher, which is an encryption technique that works on streams of data at either the character or even bit level.

A user would want to adopt this technique for example if they were sending credit card details over the Internet. If the details were not encrypted then their credit card details would be open for fraudulent use by eavesdropping entities.

By adopting some form of encryption and decryption algorithm a system is able to ensure a certain level of confidentiality to its users by protecting information. By implementing this a fifth generation system would be able to provide a level of communication and data privacy.

6.1.3 Anonymity

Another technique for preserving privacy is Anonymity. Anonymity is the state of being not identifiable within a set of subjects, the anonymity set which is a set of all possible subjects who might cause an action [Pfitzmann, 2000].

According to Pfitzmann et al. there are three types of anonymous communication properties that can be provided: sender anonymity, receiver anonymity and unlinkability of sender and receiver [Pfitzmann, 1987].

By having anonymity a user is able to conduct their affairs safe in the knowledge that their actions, location and data are still private. For example a work colleague of Bob discovers that Bob is fraudulently using company letterhead. To protect the company this work colleague reports Bob. If anonymity is not provided then this colleague could effectively be traced and identified. By ensuring anonymity in this situation the system would be providing behavioral privacy.

Li claims all of the anonymity areas mentioned by Pfitzmann et al. are being applied in her fifth generation messaging system through the use of Temporary Identities (TID) to provide anonymity in conjunction with a user's privacy.

By providing anonymity a system is providing a method to help ensure behavioral and location privacy also known as location anonymity that will now be discussed in further detail.

6.1.3.1. Location Anonymity

Location anonymity is allowing a user's location to remain unknown unless they wish to reveal those details.

The inclusion of a presence awareness system (see Section 3.2.4) would see the need for this kind of security to be in place for users. For example if a user of a fifth generation system wished to have a meeting with a prospective employer, they would probably wish to be able to conduct it without the

knowledge of their current employer. They would prefer the ability to hide information regarding action and location. From this example it is clear a fifth generation must provide location anonymity to a user.

In a proposed automated verification framework Godefroid et al. suggest a model that will ensure privacy in presence aware systems [Godefroid, 2000]. This verification framework can detect violations of complex policies using a tool called Verisoft that provides systematic tests of concurrent systems and run-time monitoring. Li's thesis did not examine this framework.

A fifth generation system must implement either this tool or provide some assurance of location anonymity / location privacy for its users.

6.2. Integrity

In any messaging system, the system must be able to ensure integrity of information, both information stored in the system and information communicated with other systems.

Integrity of information refers to the protection of information against unauthorised modifications [Li, 2001]. Integrity and confidentiality of information can affect a large number of people and corporations if it is compromised. For example Bob might accidentally send an email containing confidential information regarding a client, say financial documents. If these were altered and received by the incorrect people then fraudulent procedures could ensue endangering the reputation of Bob, his firm and the client.

Li adopts several methods to provide this integrity to users. These methods include:

- Access Control Services to protect system resources against unauthorised use.
- Non-repudiation services to provide protection against the originator of a message or action from denying that he or she has originated

the message or action as well as the recipient of the message denying that the receiver received the message.

The final area of security examined is that of Availability of Service.

6.3. Availability of Service

If a required service is not available, frustration and loss of work can often result. In a business environment this can be a costly experience. A system must be designed to prevent this non-availability of service from happening. Availability of Service can be effected in a system in a number of ways including power failure, virus or worm corruption and denial of service attacks. In her thesis Li identifies this area of Security but does not go into detail about its inclusion in the system.

Standard measures to prevent this non-availability of service include:

- Generator systems to prevent loss due to power failure.
- Fail safe software should a system crash or power loses.
- Recovery method systems to prevent or reduce data lose.
- Relevant firewalls and proxies.
- Updated virus protection systems.
- Implementation of router filters to reduce exposure to certain denial-of-service attacks.
- Disable any unused or unneeded network services, limiting the ability of an intruder to take advantage of services to execute a denial-of-service attack.
- Enable quota systems.
- Routinely examine physical security with respect to current needs.
- Invest in and maintain "hot spares" - machines that can be placed into service quickly in the event that a similar machine is disabled.
- Invest in redundant and fault-tolerant network configurations.
- Establish and maintain appropriate password policies.

[CERT, 1999]

As we can see there are several areas to security that must be examined and provided in a system that could be implemented in today's market.

The fifth generation system proposed by Li has been examined and discussed however there are still several issues that have not been examined. For correct implementation these issues would need to be dealt with to provide a functional fifth generation messaging system. These issues are mentioned next in the Future Works Section of this paper.

7. Future Works

As with all areas of technology, as systems continue to develop and evolve ensuring messaging systems designs are kept up to date and at the forefront of the market becomes increasingly difficult. Several areas of the fifth generation system still have not been addressed and as mentioned in Li's thesis, the following areas still need to be examined:

- *Service mobility*, the seamless mobility across different devices during a service session.

- *Full range of anonymity*, giving a user a full selection of anonymity.

- *Implementation*, the scale of tasks required to implement a fifth generation model.

- *Performance evaluation*, conducting performance testing and usability evaluation of the design.

Areas identified by this paper that need to be examined due to its discussions are:

- *Integration*, integrating the discussed models and systems into the fifth generation model, such as the presence awareness, billing and Ioannidis' SPA systems mentioned in Sections 3.2.4, 5.4 and 5.4.2 respectively.

- *Bayesian Filtering Discussion*, examining Graham's Bayesian filter for implementation possibilities with the persona identification concept mentioned in Section 5.4.1.

- *User Interface Development*, discussing the proposed interface with the Microsoft Corporation and determining an appropriate implementation within the system.

- *Billing Implementation*, examining Fahlmann's proposed system in more detail and determine the possibility of its incorporation.

The evaluation and discussion of these issues will see the development of the current system and possibly identify a new generation of messaging systems. Continuous adaptations and developments to the discussed model will have to be made as long as technology continues to advance.

8. Conclusion

In this paper four problems associated with messaging systems have been presented and discussed. To give a clearer understanding, existing messaging systems to date have been examined and the relationship of the four problems with the system is discussed. In particular the fifth generation messaging system model proposed by Li. The main focus of this paper was investigating the persona problem mentioned in Li's thesis.

The first step in this investigation was clarifying and redefining this problem, which was undertaken in Section 2.2.5. From here the persona identification concept was examined as a functionality that should be available to users of a fifth generation system. With this in mind a design and possible implementation of the persona identification concept was presented. These designs and the use of persona concepts in systems today (instant messaging) show how this persona identification is an important and feasible feature for an end-user of a fifth generation messaging system. The implementations of this feature via both filter and channel implementation in an existing system show that a significant step has been taken towards a solution to the persona problem. Literature not examined by Li in this area include [Bunney, 1999], [Cherry, 2002], [Zeise, 2002], [Ball, 1997] and [LaGesse, 2001]

In her future Works Section Li mentions that the area of a User Interface needed to be examined at before an implementation of a fifth generation system would be feasible. This paper took a step toward this in Section 4 where a user interface for an electronic e-mail system incorporating the persona identification concept was presented. This was developed following guidelines presented in the [Microsoft, 1993], [Belcher, 2000] and [Galitz, 1997] literature.

In addition this paper also examined relevant literature and systems not covered by Li's Masters thesis relating to fifth generation messaging systems. One model not examined by Li, which provides the locality awareness requirement mentioned in her work is the presence awareness model discussed in Section 3.2.4. The Availability of Service from a security point of view was also discussed in further detail. The literature on these topics not covered by Li includes: [Maniatis, 1999], [Godefroid, 2000], [Grudin, 2002], [Handel, 2001] and [Stone, 2001].

As with all modern day technology, messaging systems continue to grow and develop. This paper has suggested some promising directions for the future development of a fifth generation messaging system.

9. Registered Trademarks and Copyrights used in this paper

- Microsoft® referred to within the text as Microsoft
- Microsoft® Outlook® referred to within the text as Microsoft Outlook
- Microsoft® Word© referred to within the text as Microsoft Word
- Microsoft® Excel© referred to within the text as Microsoft Excel

10. References

[New Zealand Parliament, 1993] New Zealand Parliament, *An act to consolidate and amend the race relations act of 1971 and the human rights commission act 1977 and to provide better protection of human rights in New Zealand in general accordance with United Nations Covenants and Conventions on Human Rights*, Public Law Number 93, 82, pages 1374 - 1462, Part one, 01 February 1994, 1993

[Anonymous, 2002] Anonymous, *Unified Communications*, Alcatel, Paris, France, pages 1-5, 01 October 2002

[Austen, 2003] Austen, I., "New Strategy in the War on Spammers", *New York Times*, New York, USA, 02 January, http://www.nytimes.com/2003/01/02/technology/circuits/02spam.html, 2003

[Ball, 1997] Ball, G. et al., "Lifelike Computer Characters: The Persona Project at Microsoft Research", *Microsoft Research*, http://research.microsoft.com/research/ui/persona/chapter/persona.htm, Access Date: 27 November 2002, 1997

[Barich, 2001] Barich, T., *Outlook 2002: The Complete Reference*, McGee, Mike, 1st Edition, Osborne/McGraw-Hill, California, USA, 2001

[Belcher, 2000] Belcher, M. et al., "User Interface Design", *Desire Information Gateways*, http://www.desire.org/handbook/2-9.html, Access Date: 03 December 2002, Last Updated: 20 April 2000, 2000

[Bunney, 1999] Bunney, W., *Multiple Personality Internet Account*, United States Patent, USA, Sony International (Europe), Patent Date: 26 November 2002, 1999

[CERT, 1999] CERT, "Denial of Service Attacks", *(Computer Emergency Response Team), Tech Tip*, http://www.cert.org/tech_tips/denial_of_service.html, "Copyright

1997,1999 Carnegie Mellon University", Access Date: 11 Jan 2003, Last Updated: 04 June 2001, 1999

[Cherry, 1953] Cherry, C., "A History of the Theory of Information", *IEEE Transactions on Information Theory*, Vol. 1, Issue 1, pages 22-40, February, 1953

[Cherry, 2002] Cherry, S., "IM Means Business", *IEEE Spectrum*, pages 28-32, November, 2002

[Christein, 2002] Christein, H. et al., "A General Purpose Model for Presence Awareness", Plaice, J, *Lecture Notes in Computer Science*, Berlin, Germany, Springer-Verlag, pages 24-34, 2002

[DiamondCluster, 2001] DiamondCluster, "Presence Awareness: Optimizing the Marketplace", *Viewpoint*, http://www.diamondcluster.com/work/whitepapers.asp, 2001

[Fahlmann, 2002]Fahlmann, S., "Selling Interrupt Rights: A way to control unwanted e-mail and telephone calls", *IBM Systems Journal*, Vol. 41, Issue 4, pages 759-766, 2002, 2002

[Flynn, 2001] Flynn, N., *The ePolicy Handbook*, 1st edition, AMA Publications, New York, USA, 2001

[Galitz, 1997] Galitz, W., *The Essential Guide to User Interface Design: An introduction to GUI design principles and techniques*, Editor: Elliot, Bob, 1st Edition, John Wiley & Sons, Inc., Canada, 1997

[Geist, 1998] Geist, M., "A Brief Introduction to C. G. Jung and Analytical Psychology", *C G Jung Organisation*, http://www.cgjungpage.org/articles/geist1.html, Access Date: 28 November 2002, Last Updated: 7 May 2000, 1998

[Godefroid, 2000]Godefroid, P. et al., "Ensuring Privacy in Presence Awareness Systems: An Automated Verification Approach", *ACM Conference on Computer Supported Cooperative Work*, Philadelphia, USA, ACM, pages 59-68, 2000

[Graham, 2003] Graham, P., "Better Bayesian Filtering", *Proceeding of the 2003 Spam Conference*, Massachusetts, USA, MIT, http://spamconference.org/proceedings2003.html, 21 January, 2003

[Grudin, 1994] Grudin, J., "Computer-supported cooperative work: history and focus", *IEEE Journal*, Vol. 27, Issue 5, pages 19-26, May, 1994

[Grudin, 2002] Grudin, J. et al., "Personas: Practice and Theory", http://research.microsoft.com/research/coet/Grudin/Personas/Pruitt-Grudin.pdf, Access Date: 28 November 2002, Last Updated: 2002, 2002

[Hall, 1998] Hall, R., "Channels: Avoiding Unwanted Electronic Email", *Communications of the ACM*, Vol. 41, pages 88-95, March, 1998

[Halsall, 1998] Halsall, F., *Data Communications, Computer Networks and Open Systems*, 4th Edition, Addison-Wesley Publishers Ltd., Essex, UK, 1998

[Handel, 2001] Handel, M., "Presence Awareness & Instant Messaging: Multiple Devices, Multiple Endpoints", *University of Michigan*, http://www-personal.si.umich.edu/~handel/research/rvm/documents/Handel-DocConsort.pdf, Access Date: 28 November 2002, Last Updated: 2001, 2001

[Hughes, 1998] Hughes, L., *Internet e-mail: protocols, standards, and implementation*, 1st Edition, Artech House Inc, Norwood, Massachusetts, USA, 1998

[Ioannidis, 2003] Ioannidis, J., "Fighting Spam by Encapsulating Policy in Email Addresses", *The 10th Annual Network and Distributed System Security Symposium*, San Diego, California, USA, 5-7 February 2003, 2003

[LaGesse, 2001] LaGesse, D., "Instant Messaging Phenom is, Like Way Beyond Email", *USNews.com*, 03 May 2001, http://www.usnews.com/usnews/nycu/tech/articles/010305/nycu/im.htm, 2001

[Li, 2001] Li, J., *A Fifth Generation Messaging System*, Computer Science Dept.,, University of Auckland, Auckland, New Zealand, pages 161, 2001

[Maniatis, 1999] Maniatis, P. et al., "The Mobile People Architecture", *ACM SIGMOBILE Mobile Computing and Communications Review*, Vol. 3, Issue 3, pages 36-42, July, 1999

[Microsoft, 1993] Microsoft, *User Interface Design Guidelines*, Microsoft Ltd, Berkshire, UK, pages 1-14, December, 1993

[Oppliger, 1996] Oppliger, R., *Authentication Systems for Secure Networks*, Artech House, Boston, New York, USA, 1996

[Peltier, 2002] Peltier, T., *Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management*, Bryson, Lisa, 1st edition, CRC Press LLC, Boca Raton, Florida, USA, 2002

[Pennington, 2001] Pennington, B., "Authentication and Session Management: Session replay", *OWASP (The Open Web Application Security Project)*, http://www.owasp.org/asac/auth-session/replay.shtml, Access Date: 29 January 2003, Last Updated: 2002, 2001

[Pfitzmann, 1987]Pfitzmann, A. et al., "Networks Without User Observeability", *Computers & Security*, Vol. 6, Issue 2, pages 158-166, April 1987, 1987

[Pfitzmann, 2000]Pfitzmann, A. et al., "Anonymity, Unobservability, and Pseudonymity - A Proposal for Terminology", *Lecture Notes in Computer Science*, Vol. 2009, pages 1-9, 2001, 2000

[Stone, 2001] Stone, A., "Presence Awareness", *Commerce Times*, USA, 21 February 2001, http://www.mcommercetimes.com/Technology/89, 2001

[Van der Meer, 1999] Van der Meer, S. et al., "An Approach for a 4th Generation Messaging System", *Autonomous Decentralized Systems, 1999. Integration of Heterogeneous Systems Proceedings, The Fourth International Symposium*, Tokyo, Japan, Technical University, Berlin, pages 158-167, 21 March 1999, 1999

[Zeise, 2002] Zeise, A., "Developing Your Online Persona", *A to Z Home's Cool, Homeschooling*, http://www.gomilpitas.com/homeschooling/articles/063002.htm, Access Date: 28 November 2002, Last Updated: 30 July 2002, 2002

[Zimmermann, 1992] Zimmermann, H., *Fuzzy Set Theory and its Applications*, 2nd Edition, Kluwer Academic Publishers, Massachusetts, USA, 1992