

Advanced Access Control in support of Distributed Collaborative Working and De-perimeterization

A thesis submitted in partial fulfilment of the requirement for the degree of
Doctor of Philosophy

Peter Richard Burnap

September 2009

Cardiff University

School of Computer Science

UMI Number: U585408

All rights reserved

INFORMATION TO ALL USERS

The quality of this reproduction is dependent upon the quality of the copy submitted.

In the unlikely event that the author did not send a complete manuscript and there are missing pages, these will be noted. Also, if material had to be removed, a note will indicate the deletion.



UMI U585408

Published by ProQuest LLC 2013. Copyright in the Dissertation held by the Author.
Microform Edition © ProQuest LLC.

All rights reserved. This work is protected against
unauthorized copying under Title 17, United States Code.



ProQuest LLC
789 East Eisenhower Parkway
P.O. Box 1346
Ann Arbor, MI 48106-1346

Declaration

This work has not previously been accepted in substance for any degree or award, and is not concurrently being submitted in candidature for any degree or other award.

Signed 01 DEC 2010 (Candidate)

Date 

Statement 1

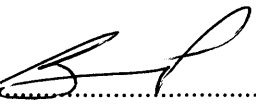
This thesis is being submitted in partial fulfilment of the requirements for the degree of Doctor of Philosophy.

Signed  (Candidate)

Date 01 DEC 2010

Statement 2

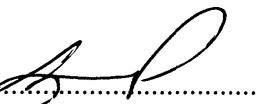
The work submitted is the result my own work/investigation, except where otherwise stated. Other sources are acknowledged by explicit references.

Signed  (Candidate)

Date 01 DEC 2010

Statement 3

This thesis, if successful, may be made available for inter-library loan or photocopying (subject to the law of copyright), and the title and summary may be made available to outside organisations.

Signed  (Candidate)

Date 01 DEC 2010

Table of Contents

Chapter 1 - Introduction.....	3
1.1. Background and Motivation for Research.....	4
1.2. Developing a Framework for Access Control.....	7
1.3. Hypothesis.....	13
1.4. Research Methodology	13
1.5. Contribution to Information Security	14
1.6. Arrangement of Thesis	15
Chapter 2 - Electronic Information Management	17
2.1. Virtual Organisations.....	18
2.1.1. Service Oriented Architecture.....	19
2.1.2. Web Services.....	20
2.2. Collaborative Information Management: The Problem Defined	21
2.3. Threat Model.....	27
2.3.1. Risk Assessment.....	27
2.3.2. System Threat Model	29
Chapter 3 - Access Control Models.....	31
3.1. Multi-Level Security Models.....	31
3.2. Multi-lateral Security Models	35
3.3. Desirable Features of an Access Control Model for Collaborative Distributed Working.....	37
Chapter 4 - Existing Access Control Technology	40
4.1. Access Control Techniques	40
4.2. Access Control Administration.....	45
4.3. Access Control Technologies.....	47
4.3.1. Confidentiality, Integrity and Identity in Distributed Systems.....	47
4.3.1.1. Achieving Confidentiality.....	47
4.3.1.2. Achieving Integrity.....	49
4.3.1.3. Achieving Confidence in Identity.....	50
4.3.2. Existing Approaches to Access Control in VOs.....	51
4.3.2.1. Defining and Enforcing Access Control.....	51
4.3.2.2. The Centralised Perimeterized Approach.....	54
4.3.2.3. The Decentralised Perimeterized Approach.....	56
4.3.2.4. Limitations of the Perimeterized Approach.....	57
4.3.2.5. Granularity of Access Control.....	59
4.3.2.6. Managing Loss of Control.....	63
4.4. Summary.....	68
Chapter 5 - An Enhanced Approach to Access Control for VOs.....	71
5.1. Achieving the Link that Obeys the De-perimeterized Linkage Rule	72
5.2. De-Perimeterized Security - Architectural Components	74
5.2.1. Information Classification Scheme.....	75
5.2.1.1. Implementing the Granular Access Control Formula	83
5.2.2. Access Control Policy Generation	86
5.2.3. Access Control Policy Enforcement	87
5.2.3.1. Implementing the De-perimeterized Access Control Formula and De-Perimeterized Linkage Rule	88

5.3.	Management of Information within the Application	91
5.3.1.	Policy Versioning	92
Chapter 6 - Evaluation		94
6.1.	Testing Strategy	94
6.1.1.	Testing Scenario	96
6.1.2.	Testing Environment.....	98
6.2.	Test Scripts	100
6.2.1.	Test Phase 1 – Advanced granularity of control over information.....	101
6.2.2.	Test Phase 2 – Enforcement of Access Control in De-perimeterized Environments 107	
6.2.3.	Test Phase 3 – Modification of Access Control Policy following Distribution.....	115
6.3.	Position to Existing Technology	118
6.4.	Risk Assessment	120
6.5.	Summary.....	124
Chapter 7 - Conclusion		126
7.1.	Contributions	129
7.2.	Future Work	131

Acknowledgements

I would like to thank my supervisors Professor Alex Gray and Professor John Miles for their guidance throughout the period in which I have been working towards this thesis. It has been a long journey!

I met Jeremy Hilton halfway through this journey and he offered me the most eye opening opportunities, opened doors that led to academic and commercial experience that most PhD students could only dream of, and helped me develop a confidence such that I have presented my ideas and gained the confidence of some of the key experts in my subject area. Thanks so much, Jeremy.

Thanks to my Dad for supporting me all the way through University and long after, while I completed this work.

Most importantly, thanks to my wife, Katherine, who has always been there to talk to and support me throughout the journey. The thesis journey ends, but ours continues!

This is dedicated to “Team Burnap” ☺

Table of Abbreviations

AA - Attribute Authority

AC - Attribute Certificate

ADS - Access Control Decision Function

AEF - Access Control Enforcement Function

CA - Certificate Authority

De-P – De-perimeterisation

DRM – Digital Rights Management

IS – Information System

PDP - Policy Decision Point

PEP - Policy Enforcement Point

PKI - Public Key Infrastructure

PMI - Privilege Management Infrastructure

PSP - Policy Storage Point

SoA - Source of Authority

SOA – Service Oriented Architecture

VO – Virtual Organisation

Glossary of Terms

Authentication	The process of confirming an identity as it is portrayed
Authorization	The process of defining whether an action is allowed for a given identity
Availability	The requirement for information to be available for access when required, without delay.
Confidentiality	The principle of restricting access to information to those who have been granted access by its owner
Integrity	The principle of restricting modification of information to those who have been granted rights to do so by its owner
Usability	The ease with which something can be used to achieve a specific goal
Usable	The ability for something to be used for a specific goal without hindrance and excessive complication. See also, Usability

Abstract

This thesis addresses the problem of achieving fine-grained and sustained control of access to electronic information, shared in distributed collaborative environments. It presents an enhanced approach to distributed information security architecture, driven by the risks, guidelines and legislation emerging due to the growth of collaborative working, and the often associated increase in storage of information outside of a secured information system perimeter.

Traditional approaches to access control are based on applying controls at or within the network perimeter of an information system. One issue with this approach when applying it to shared information is that, outside of the perimeterized zone, the owner loses control of their information. This loss of control could dissuade collaborating parties from sharing their information resources. Information resources can be thought of as a collection of related content stored in a container. Another issue with current approaches to access control, particularly to unstructured resources such as text documents, is the coarse granularity of control they provide. That is, controls can only apply to a resource in its entirety. In reality, the content within a resource could have varying levels of security requirements with different levels of control. For example, some of the content may be completely free from any access restriction, while other parts may be too sensitive to share outside of an internal organisation. The consequence being that the entire resource is restricted with the controls relevant to the highest level content. Subsequently, a substantial amount of information that could feasibly be shared in collaborative environments is prevented from being shared, due to being part of a highly restricted resource.

The primary focus of this thesis is to address these two issues by investigating the appropriateness and capability of perimeter security, and entire-resource protection, to provide access control for information shared in collaborative distributed environments.

To overcome these problems, the thesis develops an access control framework, based on which, several formulae are defined to clarify the problems, and to allow them to be contextualised. The formulae have then been developed and improved, with the problem in mind, to create a potential solution, which has been implemented and tested to demonstrate

that it is possible to enhance access control technology to implement the capability to drill down into the content of an information resource and apply more fine-grained controls, based on the security requirements of the content within. Furthermore, it is established that it is possible to shift part of the controls that protect information resources within a secure network perimeter, to the body of the resources themselves so that they become, to some extent, self protecting. This enables the same controls to be enforced outside of the secure perimeter.

The implementation is based on the structuring of information and embedding of metadata within the body of an information resource. The metadata effectively wraps sections of content within a resource into containers that define fine-grained levels of access control requirement, to protect its confidentiality and integrity. Examples of the granularity afforded by this approach could be page, paragraph, line or even word level in a text document. Once metadata has been embedded, it is bound to a centrally controlled access control policy for the lifetime of the resource. Information can then be shared, copied, distributed and accessed in support of collaborative working, but a link between the metadata and the centrally controlled policy is sustained, meaning that previously assigned access privileges to different sections of content can be modified or revoked at any time in the future.

The result of this research is to allow information sharing to reach a greater level of acceptance and usage due to:

- i. the enhanced level of access control made possible through finer-grained controls, allowing the content of a single resource to be classified and restricted at different levels, and
- ii. the ability to retain sustained control over information through modifiable controls, that can be enforced both while the information is stored on local information systems, and after the information has been shared outside the local environment.

Chapter 1 - Introduction

In both academia and industry, information is frequently shared between consortia and individuals who work collaboratively for the duration of a project. Collaborative working arrangements can have a dynamic lifespan, with users, roles, and the access control requirements of shared information resources changing at any time from project inception to completion. During that time, the owner of a shared information resource (resource owner) may wish, or be legally required to, revoke access to content previously shared with distributed collaborators in an Internet connected environment. An Internet connected environment effectively is a set of machines that are connected through the Internet. Internet connectivity is not always permanent; machines may connect and disconnect periodically. However, we assume Internet connectivity is present for the purposes of collaboration.

A prominent characteristic of most existing access control technology is that it enforces access control for information resources at, or within, a secured network, which places a perimeter of control, often a Firewall, between the information and the external Internet connected environment. Thus, outside the perimeter, access control is unenforceable, meaning access control enforcement is not possible *after* information has been shared and moved outside the perimeter. This poses a significant problem to organisations that require the ability to retain control of their information after it has been shared and moved beyond the perimeter, and often leads to data losses or the withholding of some information that would be useful to be shared with consortia members. Additionally, as collaborative working arrangements evolve, access control rights for shared information may also change. New consortium members may be given access to shared information, while other members may leave the consortium, and have their access rights revoked. To enable this, the access control policy for shared information needs to be modified, and the changes enforced on information shared outside the perimeter. This is not currently possible. Therefore, there is a requirement to develop an approach to access control that could be implemented to enhance the capability of existing technology, to be able to support the definition, modification and enforcement of the access control policy, for information stored outside the perimeter.

Furthermore, information resources are containers for a collection of related pieces of information, which often have varying levels of security requirements. Text documents and databases are examples of information resources. Certain parts of a resource may be restricted to use within an organisation, such as personal information protected by data protection laws or unpatented intellectual property. Other parts may be non-sensitive content that could be shared with collaborating partners. It may not be trivial to remove the restricted content before sharing, as it may be mixed into sections of less sensitive content. Another prominent characteristic of existing access control technology is that it enforces access control policy on the entire-resource, and not on different sections of content within the resource. As a result, the restricted content within a resource, often means the entire resource is not shared, limiting the effectiveness, dynamism, and potential of collaborative working. This presents a requirement for an approach to access control that could enhance the functionality of existing technology, such that it can apply controls not only to the resource in its entirety, but to different levels of the content within.

This thesis focuses on addressing these requirements, and aims to provide an approach to access control more suitable for supporting the sharing of information in distributed collaborative working environments, by developing a framework which supports these requirements and could theoretically be implemented to enhance existing access control technology. Because the drivers for this research stem from collaborative working involving text-based documents, the research and its results are applied specifically to text-based documents for the purpose of exemplifying and testing the suggested approach. However, the conclusions in Chapter 7 give some insight as to the wider applicability of the research, including databases. The rest of this chapter outlines the background and motivation behind the research, and defines the research methodology adopted to address these requirements, before defining the hypothesis and the contributions that proving the hypothesis would make to the information security domain.

1.1. Background and Motivation for Research

The emergence of high-speed networks in support of Grid Computing [FKNT02], Service-Oriented Architectures (SOA) [PL03], Web 2.0 [Ore07], and Cloud Computing [Hay08], and

an ever increasing connection to mobile Internet [VC02], has dramatically enhanced the connectivity and data transfer potential between distributed Information Systems (IS). IS users can now use electronic devices such as PDAs, mobile phones and laptops to send and receive data through high-speed network connections and wireless communication protocols, enabling an underpinning infrastructure for collaborative working through the sharing and co-development of information resources.

Collaborative working arrangements can have a dynamic lifespan and can vary tremendously in their purpose, scope and community [CLO87, CAGL07, She00, FKT01]. Roles, users, and the access control requirements of information content shared in collaborative environments may change at any time during, or at the end of, a collaboration arrangement. Resource owners need to control access to information shared with their collaborators and, at any time, may wish, or be legally required, to revoke access to previously shared content.

A scenario that represents this kind of environment is the sharing of information from Electronic Health Records (EHRs) in the health and social care domain. A typical sharing scenario starts with a patient presenting symptoms to their GP, being assessed, and being diagnosed. A report is then written by the GP. If the symptoms present a case for further investigation, such as a painful lump beneath the skin, the GP may also write a referral letter. The referral letter will contain information such as the presented symptoms, symptom duration, location and degree of pain it is causing. The referral may require the patient to visit a hospital. The hospital would be given access to the GP's report, the referral letter and perhaps some medical history. The hospital visit may result in a scan and an associated report. If required, the patient may be referred to a second hospital, which results in a physics report. The second hospital would be given access to the GP's report and referral letter, and the scan and report from the first hospital. If a cancer is confirmed, the patient will be referred to a consultant oncologist who will write a prognosis report and write up a course of treatment, based on all the relevant information shared by the other institutions. Various other reports are generated as treatment continues. Any of these document outputs may be requested and shared between any of the healthcare professionals along the patient care path, as they collaborate to treat the patient. The GPs, clinicians, consultants and biomedical staff effectively become a collaborative consortium, working at different geographic sites within their own distributed, autonomous network perimeters.

Each institution is legally responsible for the data protection of the information they hold about a patient, under the UK Data Protection Act (1998) [DPA98]. Additionally, as Perioellis et al. [PCC+06] note, collaborative working environments are dynamic by nature and thus access rights should not be automatically assumed on inclusion in a collaborative working consortium. Rather they should be granted and removed when necessary throughout the lifetime of the collaboration. Access rights for a particular collaborator may vary depending on the task in which a collaborator is active. Therefore, if information is to be shared between organisations, there is a clear requirement for resource owners to retain management of the access control policy for information shared outside their perimeter. In the healthcare scenario, each collaborator only needs access to a patient's medical record for the duration of the patient care, and even then, they only need access to the parts of the record that are required to perform their role in the collaboration. For example, while the clinician performing a scan at a hospital might need access to the patient's medical history to determine if the patient has a medical condition that could be aggravated by the scanning process, there may be certain sensitive parts of that information such as a history of mental illness or HIV status that do not need to be shared, and would ideally be removed from the report before it is shared to limit the potential risk of its exposure. As Anderson points out [And08], there is an ongoing effort to achieve acceptance of the Electronic Patient Record (EPR) in accordance with the British Medical Association (BMA) Security Policy [And08]. The problem of how to restrict access to specific parts of patient records, such as identity, medical history, sexuality, and prescribed medication is an ongoing situation. More people now have electronic access to patient information and current technology has not managed to implement an effective means of "sealing and locking" certain parts of the patient record to provide selective restricted access to a document. There is therefore a requirement for access control to be applied to content within a resource at different levels, as well as to the resource in its entirety.

This scenario poses two key requirements to achieving the secure sharing of information in collaborative working environments: *sustained control of information* after it is shared, and *varying levels of control* over the content of a shared resource, not just the resource in its entirety. These requirements are not unique to this scenario. The concept of access control retention and limiting access to certain parts of shared resources is applicable to any organisation wishing to share information in an Internet connected environment, for which they have a responsibility, to themselves or others, to protect. Changes to the UK Data

Protection Act (1998) [DPA98] mean stricter controls and harsher penalties for data controllers who leak personally identifiable information. In addition to this, many organisations have information resources that would cause financial or reputational loss if not controlled properly, but would be useful to share with collaborators for the purpose of achieving a shared goal. Examples of this are pre-budget financial reports, ideas for new products and services, and designs for technology, machinery or new pharmaceutical drugs. All of these could be developed in distributed collaborative working environments, and could be harmful if not properly controlled. Indeed the latest Boeing aircraft can be assembled and rolled out in three days [BOE], largely due to distributed collaborative development and manufacture. The plans for the aircraft are very sensitive to Boeing but must be shared in a distributed collaborative working environment to facilitate the speed of assembly. This research is applicable to any individual or organisation that shares information with other parties, in a collaborative Internet connected environment, and has a responsibility to protect the information while it is being shared.

1.2. Developing a Framework for Access Control

These requirements are currently extremely difficult to support using existing access control technology, and provide motivation for research into enabling such support. The limitations of existing technology are discussed in a literature review in Chapter 4. However, the reasons why it is currently difficult to support these requirements are very clear from a high level overview of existing access control technology. It is possible to formulate a **basic access control framework** as follows, which aims to represent a typical current situation such as the health information sharing problem [And08] and the collaborative working environment at Boeing [BOE], as defined in Section 1.1.

Let D be a set of documents.

Let C be set of information classification schemes.

Let U be a set of users.

Let A be a set of actions (to be performed on a document).

Let R be a set of access control rules.

Within a distributed collaborative environment, it is possible to take an individual organisation's classification scheme (c_k) where $c_k \in \underline{C}$, a user (u_z) where $u_z \in U$, and assign the user a security label from the information classification scheme. This creates a user security label c_{ku} . It is possible to take a document owned by that organisation (d_x) where $d_x \in D$, and do the same, giving a document security label c_{kd} . Assuming the labels in c_k are ordered in some way, i.e. for any two labels c_{ki} and c_{kj} , where $c_{ki} \neq c_{kj}$, $c_{ki} < c_{kj}$ or $c_{ki} > c_{kj}$, both user and document labels represent security levels. The document label represents the level of security required for a user to access the information held within. The user label typically represents the highest security level for which they can obtain access. This means there will exist some relationship between c_{ku} and c_{kd} that determines whether access should be granted or denied. These relationships are expressed using rules, defined by the organisation. A set of access control rules (r_b) where $r_b \subseteq R$, as defined by the organisation, can be defined to support access control decisions and restrict user access to a document. Using elements from the basic access control framework, we can express perimeterized access control decisions as a function $f(c_{ku}, c_{kd}, a_i, r_b)$, where the function is passed a user label c_{ku} , the target document label c_{kd} , the requested action a_i , where $a_i \in A$, and set of rules r_b , as input parameters. The function then determines if the requested *action* is allowed or denied by evaluating the set of access control rules defined by the organisation (r_b), and a result of 'allow' or 'deny' would be returned. For example, if an access control rule (r_{bi}) states that the user's security label must be greater than that of the document in order to gain read access, i.e. r_{bi} where $r_{bi} \in r_b = c_{ku} > c_{kd}$, an invocation of the function with input parameters $c_{ku} = \text{Level0}$ and $c_{kd} = \text{Level1}$, would result in an output of *deny* because Level0 is not greater than Level1. Access control rules are explained in further detail in Chapter 3.

However, assigning a security label c_{kd} to a document d_x . means the entire document is classified at a single level. This assumes that the user, should they meet the requirements of the access control rules, is able to access the entire document, and that all content within the document has the same security requirements. This is often not the case. For example, take the Electronic Patient Record (EPR) sharing scenario. The record comprises demographic patient details, medical history, current and previously taken medication, and long-term illness details. The information owner, for example a GP, may wish to share some of this information with a local hospital when referring a patient. Or, from a global view, a patient may become ill while abroad and the local hospital may require access to an EPR to understand a patient's reaction to a particular treatment. The GP, and in fact the patient, may

not wish to share the entire record. Long term illness such as HIV or previous medication for depression is not relevant to anyone other than the GP and could be damaging to the patient's reputation if exposed. For this reason, only part of the document should be shared. The basic access control framework cannot support access control beyond a document in its entirety and for that reason becomes inappropriate at this point for information shared in distributed collaborative environments. An investigation is needed to extend the framework to support a more granular level of access control.

A major limitation relating to the sustained control of information after being shared with collaborators is the current approach taken to providing access control. Traditional approaches to access control are based on a *perimeterized* approach. Documents are stored inside secured perimeters and access control is enforced at, or within, the perimeter. Network perimeter technology is the most commonly used barrier between users and information. An organisation will set up its information system, store all its information resources and access control rules on local disks and servers within a local area network and deploy controls such as firewalls that control incoming and outgoing connections at the network perimeter to protect the information held within. According to the BERR 2008 survey conducted by Price Waterhouse Coopers [BERR08], 98% of organisations use this approach. However, a distributed collaborative information-sharing environment is inherently detrimental to the security of information secured using the perimeterized approach, because to share information the documents often have to leave organizational perimeters, rendering the access control technology used to protect the documents ineffective. For example, if a GP e-mails an EPR to a clinical consultant at a hospital, or gives them access to an online repository from which the EPR can be downloaded, the document that comprises the EPR moves from within the GP's perimeter to the hospital's perimeter which, by definition, means the perimeterized controls used to restrict access within the GP's perimeter cannot be used to enforce access control rules.

The identification of this as an issue is supported by the number of reported recent information exposures and losses, including 25 million personal records lost by Her Majesty's Revenue and Customs (HMRC), due to careless control or theft of remote working devices such as laptops, portable storage drives and mobile phones [BBC07a], [BBC07b], [Esp08], [BBC08a], [BBC08b], [Cor08]. This evidence further increases the pressure and need to retain control over distributed information. The interim solution within HMRC, as outlined in the Transformational Government annual review [HMG07], has been to put a

complete ban on the transfer of bulk data without adequate security, such as encryption, and to disable the downloading of information onto removable media unless a senior manager overrides this for critical purpose. The same report details that the Crown Prosecution Service (CPS) has done something similar, needing the explicit permission of the IT security officer to download information to removable media. These are organisations that need to share information outside their perimeters for audit and case working processes, but are now heavily restricted because of recent data losses.

To extend the framework to represents this issue, we need to introduce the concepts of domains, perimeters and enforcement controls.

A perimeter in this context is the interface between Internet-connected users and organisation-owned documents. This is typically deployed at the gateway to an organisation's network.

A domain in this context comprises a subset of all perimeters that have a common and agreed information classification scheme and set of access control rules. For example, a domain could be a collection of organisations with common national purpose such as hospitals within the National Health Service or Government departments, or a wider international purpose such as the G8 forum.

An enforcement control in this context is a technology that makes *decisions* on whether to allow or deny document access to a user, and *enforces* the decision.

Thus,

Let I be the set of all machines connected to the Internet

Let M be the set of all domains within the Internet

Let P be the set of all perimeters

Let E be the set of all enforcement controls

This thesis is focused on information security in distributed collaborative computing environments; therefore, we can assume that this environment contains all machines that are connected to the Internet. Thus, our applicable environment is I .

All organisations have perimeters. All domains have perimeters. However, a domain can be a subset of all perimeters, when comprised of several organisations.

Perimeters are used to manage access to information held within them. They contain documents managed by the organisation, rules defined to control access, and enforcement controls to make access control decisions and enforce them. A given organisation's perimeter therefore can be formulated as $P_a = \langle \{d_1 \dots d_n\}, \{r_1 \dots r_n\}, \{e_1 \dots e_n\} \rangle$, which represents a perimeter containing a subset of all documents, rules and enforcement controls.

With the perimeterized access control approach, documents depend on the perimeter to mediate between users and enforcement controls to ensure access is not granted to documents without a user being authorized by the enforcement control. The mediation works by a user sending an access request to an interface at the perimeter of the organisation that stores the documents. The request will include the document identifier (d_x), the user's identity (u_z) and a requested action (a_i), for example 'read' or 'write'. The perimeter interface will invoke an enforcement control from the set $\{e_1 \dots e_n\}$, to make the access control decision for a document d_x , using rules from the set $\{r_1 \dots r_n\}$. The first job of the enforcement control is to look up the user and document security labels from their identifiers. The access control decision function $f(c_{ku}, c_{kd}, a_i, r_o)$ is then used to make that access control decision, being passed the user and document labels, requested action, and set of rules to use when making the decision. The decision is then enforced by the enforcement control. The key issue with this approach is the reliance on the perimeter interface to ensure the enforcement control is invoked, and the requirement for the access control decision function to know where to find the set of rules to use. If the document is not within the perimeter, the enforcement control can be bypassed. Even if the control is enforced, and it attempts to invoke the access control decision function outside the perimeter, the function would not know where to find the rules to use to make its decision. The decision function cannot be executed outside the perimeter, unless the user label (c_{ku}), document label (c_{kd}) and set of rules (r_o) are able to be interpreted and enforced within a different perimeter. To achieve this requires an agreed information classification scheme and set of access rules between perimeters, something characteristic of a domain in the context defined above, but something that seldom exists outside of pre-defined domains.

A domain M is effectively a subset of all perimeters. That is $M \subseteq P$. Domain subsets of P can be exempt from the problems of the perimeterized access control approach because they can agree a shared classification scheme and set of rules, which means they can interpret user and

document labels, implement the access control decision function, and enforce the rules between its perimeters.

However, domains are difficult to construct between organisations that deal with very sensitive information but need to share information to collaborate, such as GPs and hospitals, or the organisations that collaborate in the design of Boeing aircraft, where the concern is the exposure of information such as personal information protected by data protection laws or unpatented intellectual property. The information owner must remain in control of who accesses this information, and thus, in control of the set of rules that govern its access. This means the set of rules of an organisation (r_o) must remain within the owner's perimeter, to prevent anyone modifying them. Thus, the perimeterized approach cannot support information sharing in distributed collaborative environments because the access control rules cannot be enforced by the access control function of another perimeter, without leaving the control of the information owner. Thus, sharing information outside the perimeter becomes very limited.

To combat this, a study is required into how perimeterized access control functionality can be configured more appropriately, such that the enforcement of access control rules is available to support the situation where a document moves outside the perimeter, as it would in a distributed information-sharing scenario, but where the rules remain under the control of the owner so that they can manage and modify the access control policy to their requirements.

The main aim of this research is to define an advanced framework that will provide a platform for the enhancement of existing access control approaches, to allow individuals and businesses to share information required for collaboration where, previously, limitations in technology may have restricted their ability to share such information, due to: small amounts of highly restricted content in a resource raising the classification of the entire resource or; the requirement to retain sustained control over the information to comply with data protection laws. Also, to reduce the likelihood of the kind of information exposures and losses that have been reported recently.

The motivation for this research, based on observations of real-world security breaches and scenarios, indicates that important issues needing to be addressed are:

- Enabling the refined, granular classification and labelling of information that reflects varying levels of content security requirements within an information resource.

- Defining, modifying and enforcing access control policy on information shared outside the perimeter in distributed collaborative Internet connected environments.

1.3. Hypothesis

The hypothesis of the research is as follows.

A document's content can have security enforced at different levels of granularity within the overall document, and the rules defining its access control are always modifiable and enforceable in an Internet connected environment, no matter where the document is held.

1.4. Research Methodology

A literature review will investigate how to enforce controls outside the secure network perimeter by analysing how existing work applies access controls inside the perimeter, and then identifying how to extend this to allow them to be applied outside the traditional perimeter of control. The review will focus on how well current access control models and technology support the owner of an information resource in the protection of their information, identifying shortcomings in current approaches and looking at what can be done to improve support for the owner from an access control point of view. Furthermore, from a collaboration information security perspective, it will also investigate the extent to which currently implemented access control technologies support collaborative working, focussing on information security once access has been granted to a collaborating partner, and how this can be sustained in distributed collaborative environments. This includes the current levels of access control granularity available for an information resource, that is, how far the owner can drill down into their resource to apply access control restrictions, and the current ability to retain control of information after it has been shared.

If information is to be protected at finer levels of granularity, then there is a need to classify information content at different levels, in order to apply the proposed protection to it. Research into classification schemes, both governmental and commercial is important, as it will inform the development of a classification scheme for use in information sharing, and investigate the possibility of a common format for representation of information classification labels.

To get a clear understanding of the business, legal and technological motivation behind existing methods and approaches, the literature review will take a bottom up approach. This will begin with an investigation of the early security methods published some thirty years ago, and build on these foundations to determine, through risk assessment, the emerging risks associated with the development of contemporary distributed collaborative working environments. Supporting mechanisms such as standards and best practice currently used for access control, methods for securing information in situ and in transit, information classification schemes, and handling proprietary documents across distributed, homogenous systems, will be considered against current approaches.

The limitations of existing technology and the resulting risk to information, identified from the literature review, will define a system threat model, which will be the basis of a requirements definition for an extension of the basic access control framework that is better suited to the modern collaborative working approach.

To test the feasibility of implementing the resulting framework, a prototype application will be developed that will attempt to codify the formulae and rules that emerge through the research. Once implemented, the system threat model will be used, together with the initial hypothesis, to evaluate whether or not the extended framework can be used to support the statement in the hypothesis, and mitigate the threats identified in the threat model. This will identify weaknesses in the framework and the prototype and perhaps identify other risks and issues that were not captured in the initial risk assessment.

1.5. Contribution to Information Security

The major contribution of this thesis is a framework that supports i) the concept of granular information classification, to the content level within a document, rather than being limited to the document in its entirety, and ii) the concept of a de-perimeterized approach to access control enforcement, such that access control policy can continue to be modified and enforced, even after information has been shared outside an organisation's perimeter and stored anywhere in an Internet connected environment. The framework enables resource owners to identify sensitive sections in their information resources and apply multiple classification labels to content within the resource, in addition to classifying the resource as a single entity. The framework also enables resource owners to retain access control of their information, even after it has been shared outside the perimeter. Retention of access control

allows changes in security requirements to be enforced on information that has already been shared, enabling revocation of access to some parts of a resource, or complete redaction of the information to occur, no matter where the resource is stored or how many times it is replicated.

The framework has been implemented in a prototype application. The application has been used to test the feasibility of the framework. That is, to prove that it is possible to codify the concepts of the framework and implement its functionality. If the framework is applicable to an individual's research agenda or security requirements, the application itself can be considered a contribution.

1.6. Arrangement of Thesis

The thesis presents the understanding of the problem, an analysis of electronic information management, existing access control models, techniques and technology, a risk assessment and derivation of a system threat model as a requirement specification for new access control technology, and the development and implementation of new technology in response to this problem, thereby supporting the claims of the hypothesis.

Chapter 2 gives an understanding of the nature and purpose of collaborative working environments, together with a risk assessment and system threat model for information sharing in such environments. It details recent information exposure cases and the responses from governing bodies to these cases by the introduction of new legislation and reconsideration of the way people work and collaborate in the light of this. Finally, it identifies the personal and business drivers for an advanced approach to access control that defines the need for protection against information exposure and corruption in distributed environments, as well as some of the legal issues that could arise as a result of not providing these facilities.

Chapter 3 investigates current access control methods in relation to the collaborative distributed working domain. This section is largely focussed on the development of the access control framework and forms the basis for comparison of current technologies within the framework, and emerging risk identified in collaborative distributed working environments.

Chapter 4 is an analysis of existing access control technology placed within the framework. The aim of this section is to identify the shortcomings of existing approaches to access control when considering the new framework and risks associated with the currently emerging electronic environments in the light of the complexities and requirements needed to deal with this risk.

The final part of Chapter 4 investigates the current approaches to information classification. Namely, how information content with varying levels of access restriction requirement can be assigned labels that identify the content as having a certain classification and how access to it should be restricted.

Chapter 5 details the design of a prototype application that is used to test the feasibility of implementing the framework. This builds on current information security methods and technologies, to implement a framework more capable of handling information sharing in Internet connected environments.

Chapter 6 goes on to evaluate the framework by testing the results of its implementation and identifies advantages and limitations with both the framework and the approach used to implement and test it.

Chapter 7 includes the conclusions of the research and identifies future work to be carried out.

Chapter 2 - Electronic Information Management

The emergence of high-speed networks in support of Grid Computing [FKNT02], Service-Oriented Architectures (SOA) [PL03], Web 2.0 [Ore07], and Cloud Computing [Hay08], and an ever increasing connection to mobile Internet [VC02] has dramatically enhanced the connectivity and data transfer potential between distributed Information Systems (IS). IS users can now use electronic devices such as PDAs, mobile phones and laptops to send and receive data through high-speed network connections and wireless communication protocols enabling an underpinning infrastructure for collaborative working, through the sharing and co-development of information resources. It is now feasible that in the not too distant future; people, electronic agents, services and devices may seamlessly interact with any number of IS under autonomous control [KFJG06], creating an ambient communication environment [Lin05] in which information sharing and collaboration between organisations can occur.

Innovation has led to the evolution of internal and inter-organisational business practices to support on-demand collaboration between geographically dispersed users, electronic information resources and electronic services [She00]. Enabling technology such as Web Services and Service Oriented Architecture (SOA), which will be introduced in the next section, can traverse organisational information system network perimeters allowing collaborative working through audiovisual conferencing technologies and electronic data interchange. This thesis focuses on the information security requirements and emerging risks to information shared within distributed collaborative working environments such as Virtual Organisations (VOs).

This chapter extracts the requirements for information security within collaborative working environments from the literature, and draws attention to the emerging risks associated with the nature of such environments, as new methods of collaborative working are introduced and as social attitude towards online collaboration shifts to a shared information culture.

2.1. Virtual Organisations

Foster and Kesselman, prominent researchers in collaborative distributed computing [FKT01] define a VO as a set of individuals and/or institutions that support highly controlled resource sharing. Resource providers and resource consumers in a VO clearly and carefully define exactly what is shared, who is allowed to share, and the conditions under which sharing occurs. They also define the purpose of a VO as being used for the sharing of distributed processing power in highly processor intensive applications. This was arguably the founding reason for VOs, which is in line with the development of high speed networks, and processor farms that acted as a springboard for Grid computing, high performance computing and distribution of processor intensive tasks [FKNT02]. However, the technology that emerged to enable such VOs now supports the management of ad-hoc integration and connectivity between inter-organisational, distributed, heterogeneous information systems, through a mapping of organisational roles into an electronic environment [CAGL97, Var02, PCH+06]. VO infrastructure allows information to be shared within the VO controlled domain and stored within the autonomous network perimeters of the distributed collaborating partners [Var02].

VOs can be dynamically formed and dispersed as required, thus allowing a virtual team of collaborators to allocate roles, responsibilities and resources, just as they would in a real organisation. The difference being that these organisations only exist as a virtual team formed for a particular task or activity, and the VO infrastructure supports their collaboration.

The role of a collaborator in VOs can change regularly from system-to-system with varying levels of responsibility and information access privileges [PCC+06]. The ad-hoc nature of a VO makes it difficult to define a static set of users, roles and resources upon which information security constraints can be defined. The development of the infrastructure to support VOs as a collaborative technology has created a new generation of information exchange capability. This leads to a new level of threat, new vulnerabilities, and new requirements for information protection. It is the security management during information interchange and collaborative development in VOs that drove the research described in this thesis. Thus, it is important to look at the supporting technologies for VO functionality in order to understand the transfer infrastructure for distributed information, and the vulnerabilities and threats that are present.

2.1.1. Service Oriented Architecture

Service Oriented Architecture (SOA) [PL03] is becoming well established in the distributed computing domain, as an enabler for computing applications to draw on the functionality of other computing applications across a network. The SOA architecture is based on what is known as the *publish-find-bind* paradigm as illustrated in Figure 2.1. The owner of a computing resource, also known as a service, publishes the availability and functionality of their service into a service registry, so that they can be discovered (found) by other people on the network, who can then bind to this service and utilise its functionality and so gain connectivity between disparate IS.

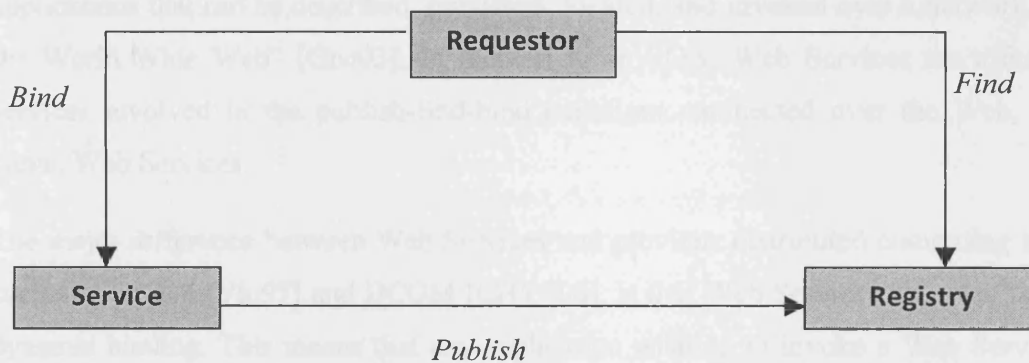


Figure 2.1 – Service Oriented Architecture

The SOA architecture spawns three major roles: Service Provider, Service Broker and Service Requestor which correspond to the publish-find-bind paradigm. SOA effectively enables, where feasible, the functionality of any particular part of a business process (including information) to be deployed on any web enabled and configured resource. This allows the business process to be decomposed into services and distributed across multiple networks and organisations. Remote services are often managed, administered and deployed by different, collaborating organisations with information being shared between the collaborating services. This configuration is a prime example of a VO in practice. Take an example of inter-organisational collaboration involving the sharing of information between organisations. The service resource could be the information itself, the requestor would be an organisation requiring access to that information, and the registry could be a list of information resources shared within the VO by each organisation. Thus, the SOA architecture is a means of supporting the dynamic sharing of information resources in VOs. However, the

sharing of information may require the transfer of information outside of the network perimeter of the organisations that own the information. The vulnerability of this lies with traditional information security being based on a perimeterized security model, which means that, while connectivity between disparate IS can be achieved, controls cannot be applied to information after it has been shared in this way and has moved outside the perimeter. This provides motivation for research into a suitable access control model to protect information after it is shared in this way.

2.1.2. Web Services

IBM's definition of Web Services states that "Web Services are self-contained, modular applications that can be described, published, located, and invoked over a network, generally the World Wide Web" [One03]. In relation to an SOA, Web Services are effectively the services involved in the publish-find-bind paradigm, connected over the Web, hence the name, Web Services.

The major difference between Web Services and previous distributed computing technology such as CORBA [Vin97] and DCOM [CHY+98], is that Web Services use what is known as dynamic binding. This means that any application wishing to invoke a Web Service can be dynamically composed and can bind to the service upon being run for the first time. Other technologies such as CORBA and DCOM require an application wishing to invoke a distributed service to be previously aware of the binding and communication paradigms, and information input/output requirements used in the remote service. This means that applications invoking the service require the hard-coding of this information into the application, which reduces the dynamism, flexibility and adaptability of the application. Web Services use structured service descriptors published in files known as Web Service Description Language (WSDL) documents [CCMW01]. WSDLs contain the binding and communication paradigms, and input/output requirements of the service, and are made publicly available on a network so that they can be utilised when required to compose an application that invokes the service. WSDLs are structured and standardised across all Web Services meaning that Web Services are programming language and operating system independent. CORBA and DCOM are not independent, as they require prior knowledge of the remote services' object types and programming languages. The nature of Web Services makes them ideal for supporting collaborative working through an SOA in VOs. They allow organisations to communicate in real-time, without any human involvement in setting up the

communication, and the potential heterogeneity due to the operating systems and programming languages used at each end is not an issue. However, the use of Web Services also means that the information used within and between services must be dynamically accessible. This provides further motivation for research into the protection requirements of information in this situation. In earlier distributed computing activity when the binding between distributed services had to be hard coded, it was possible to identify the information required during the interaction and the users who would be using the services. This allowed the owner of the information the opportunity to apply access control restrictions to the information. With the dynamic nature of Web Services, this becomes increasingly difficult to implement since the authorised users of the services change frequently, as does the information usage. Thus, the information requirement is not obvious until the services bind. This dynamic information sharing and usage requirement motivates investigation into a suitable method for protection and access control in these situations.

2.2. Collaborative Information Management: The Problem Defined

With the increasing adoption of dynamic collaborative connectivity between IS's in VOs, comes the emerging risk of information vulnerability to exposure, and loss of organisational control over restricted information. The majority of the current access control technology (see Chapter 4) involve maintaining a secure perimeter, within which, information resources are stored. The perimeter model assumes intense, scrutinised access control is enforced with a basic precept that nobody would breach that perimeter and have access to the resource, unless they have been granted the necessary permissions. The granting of access and usage permissions, or privileges, is usually dealt with by information security administrators. This group of people within an organisation are responsible for the definition and enforcement of the protection and restriction requirements for information owned or stored by the organisation. Aside from the fact that the network perimeter doesn't always stand up to intruder hits [BERR08], and control over restricted information can be lost despite these preventative measures, the adoption of collaborative working environments and dynamic VO formation has meant that information must be shared and accessed outside the network perimeter, to allow information to be shared with the right people at the right time to enable collaborative working [HMG08b].

The initial motivation for this research stems from work on the DTI funded COVITE project [BPJ+05] that investigated early Grid and Web Service techniques for information sharing within VOs. The VOs involved in the COVITE study were made up of collaborating members of project consortia within the construction industry. COVITE produced an infrastructure for distributed searching of heterogeneous, autonomous supplier databases to support the electronic procurement of products and services required during the lifetime of a construction project. A major concern of collaborating partners who provide information to the consortia (supplier database owners) is how much control they have over their information once it has left their systems (perimeter). They have discretionary control over who is allowed to search their databases and can restrict the tables and columns of the databases that are queried on site and want similar control when the information moves to another site. This detailed, often sensitive content is vital to the business process of the suppliers. Its protection outside of the local system and within a VO domain is an important concern when the supplier is considering its release to the VO for collaboration to occur, and this must conform to the information security requirements of the supplier. Suppliers must be able to trust the VO security infrastructure to provide the desired level of control over shared information. This level of control of information was not possible at the start of the project in 2002 or at the end of the project in 2005. Quite often, when conducting interviews with suppliers about the COVITE proposals, the response was that unless they had full control of what happened to their information outside their information system perimeter, they would not consider letting the information leave their system. This response indicated the weaknesses in current information sharing controls and how lack of continuous control over information hinders its usage in distributed collaborative working.

Recent contributions to research into access control of shared information in collaborative working, detailed in Chapters 3 and 4, have focused on enforcing controls based on a perimeterized approach, where information resources reside within a secure perimeter such as the network of an organisation or on a personal computer [WSF+03], [CO02], [TJM+99], [ACC+03]. The rules that define the users, roles and access controls to shared resources are typically developed within VOs and are enforced within a perimeter boundary.

However, for collaborative working to occur, which enables collaborators to access and contribute to information resource content, it is sometimes necessary for information to be shared outside the perimeter and stored on the information systems of fellow collaborators, as occurred in the COVITE project [BPJ+05], and is still occurring in scenarios such as

Electronic Patient Record sharing [And08], as described in Chapter 1, and in government services. The scope of information sharing in government is defined in the Information Commissioner's Data Sharing Review, 2008 [TW08] which states that personal information must often be shared to protect national security, to help prevent crime, and to identify the perpetrators of crime. In times of a heightened risk of terrorism, agencies, typically, but not necessarily in the public sector, are increasingly sharing or pooling relevant information about people identified as presenting a risk of harming others. It goes on to detail that it is self-evident that personal data must be shared in order to achieve these purposes, but that this begs questions about the scale and circumstances of the sharing. Collaborating agencies will add and modify the content of the shared information, passing the latest version of the information between them over whatever data transfer mechanisms they choose. In this scenario it becomes practically impossible to enforce perimeter-based security as the information is moved outside of the perimeter.

The UK Government is facing the same issue with its Transformational Government agenda [HMG08a], which outlines a "shared services culture" in terms of information and infrastructure, and aims to empower public service users with a greater level of control over the information held about them and available to them. Websites such as Direct.gov.uk and Businesslink.gov.uk have already been developed with the aim of creating a central point for users to access information generated and managed by many different Public service sectors. The "Data Handling Procedures in the Government" report [HMG08b] commissioned by the Prime Minister in June 2008 states that Public service delivery relies on the right information being available to the right people, while the 2007 Transformational Government Annual Report [HMG07] states that public and private sector organisations need to be able to share information securely in order to be able to provide these services. This neatly summarises the current situation with regard to information sharing. It is recognised that information needs to be shared and accessed by authorised people, often outside of a secure perimeter, in order for collaboration between organisations to occur and for efforts such as Transformational Government to succeed. At the same time, organisations need to be able to perform this sharing of information in a secure manner, which is proving to be very difficult to achieve as existing approaches to securing information when sharing information and working outside the perimeter clearly have weaknesses, as demonstrated by the number of recent news articles identifying information security breaches. Some of these are summarised in the next paragraph.

In November 2007, HM Revenue and Customs lost discs containing the personal details of 25 million people [BBC07a]. This was followed by news in December 2007 that nine NHS trusts in England had lost patient records [BBC07b]. In January 2008, four CDs containing personal details from court cases were lost by the Courts Service [Esp08]. Also in January 2008, a laptop was stolen containing the personal details of 600,000 people who had expressed an interest in, or applied to join, the Royal Navy [BBC08a]. HSBC revealed that a disc containing the details of 370,000 people had been lost in April 2008 [BBC08b]. In July 2008, it was revealed that 121 memory sticks had been missing or stolen from the Ministry of Defence since 2004, three of which contained information classified as 'secret' and nineteen contained 'restricted' information [Cor08]. These are just a selection of the reported cases, which show the wide range of national, civil, and commercial services involved. It is not down to technology alone that these losses are occurring. It is also important to consider the procedures and policies put in place within the organisations to protect information, as defined in the ISO 27001:2005 information security management specification [ISO05], and how well the employees of the organisations are educated in how to apply those procedures. However, the recent information exposure and loss due to careless control or theft of remote working devices such as laptops, portable storage drives and mobile phones, further increases the need to maintain control over distributed information outside the perimeter. The HMRC data loss prompted the development and publication of the Data Handling Procedure in Government report by the cabinet office [HMG08b]. This report defines how the UK Government has introduced new measures to protect information including the obligatory use of protective measures such as encryption, and controls for use with mobile devices and access to records. In the healthcare domain, the UK National Health Service (NHS) has also defined a National Encryption Framework and Encryption Code of Practice [NHS], mandating the use of encryption for information that is to be moved outside the perimeter. These reports are intended to protect all personal data, while recognising that some data requires a greater degree of protection than others. A significant research problem then, is how to maintain control over information outside the perimeter and how to classify information according to its required degree of protection.

In addition to the embarrassment that organisations incur when the news of data losses hits the headlines, it could be argued that the traditional approach to protecting information resources in their entirety within a network perimeter, and not effectively maintaining control of the information once it leaves the perimeter, is not a satisfactory approach to complying

with the requirements of the UK Data Protection Act (1998) [DPA98]. The DPA states that controllers of data must ensure that “measures ensure a level of security appropriate to the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage”. Perimeterized control could be seen as no longer appropriate for protecting information shared in collaborative distributed environments, as essentially there is *no* control outside the perimeter. If this were the case then it is also feasible that people could begin to take legal action against organisations that lose information held about them. Section 13, Part II of The Data Protection Act 1998 provides legislative backing for people to do just that, and states that “an individual who suffers damage by reason of any contravention by a data controller of any of the requirements of this Act is entitled to compensation from the data controller for that damage”. Currently, in the UK, repercussions facing an organisation are legislative and can enable financial punishment to be enforced. The Prime Minister has recently requested that the Information Commissioner conduct an independent review of data sharing to consider the way the Data Protection Act (1998) operates in the UK, and the options for implementing any such changes, as well as recommendations on the powers and sanctions available to the regulator and courts in the legislation governing data sharing and data protection. This report [TW08] states that an amendment to the Data Protection Act will give the Commissioner the power to impose civil penalties on any data controller (public or private) who breaches the data protection principles deliberately or recklessly. This means that the person in charge of data protection is personally liable, if there is a breach of data protection on the information they control. This is particularly relevant to the scenarios described in these first two chapters, as they involve the sharing of personal information that would be governed by the Data Protection Act.

One could argue the amendments to the Data Protection Act will create a more vigilant and security conscious information officer, but equally it could be argued that this amendment does not bode well for the uptake of information sharing while technology cannot provide an appropriate means of securing shared information. If sharing information means there is a chance a person’s finances, future employment, or even freedom are at risk, they will be much less likely to allow that information to be shared, if they cannot be certain the information will remain secure in a distributed collaborative environment. Given the recent data loses, this is evidently not a guarantee they can currently be offered. Thus, this scenario once again presents the problem of how to maintain control over information outside of the perimeter.

The interim solution within HMRC, as outlined in the Transformational Government annual review [HMG07], has been to put a complete ban on the transfer of bulk data without adequate security, such as encryption, and to disable the downloading of information onto removable media unless a senior manager overrides this for critical purpose. The same report details the reaction of the Crown Prosecution Service (CPS) who have done something similar; by needing the explicit permission of the IT security officer for downloading information to removable media.

These recent reports by HM Government, together with the COVITE and healthcare scenarios have highlighted two major points:

1. There is a desire to share information between collaborating organisations to provide more accurate and efficient provision of services. Transformational Government aims to facilitate the sharing of information between Public sector services and the population of the UK. COVITE requires the sharing of supplier data in product and service searches. In healthcare, patient information is shared between the organisations treating the patient. Thus this need is present in both public and private sectors.
2. There is not enough protection available to facilitate the sharing and storage of information outside the perimeterized information systems of these collaborating organisations. This is evident in the actions of HMRC and the CPS who, by banning the transfer of information to removable media, have effectively put a definite limit on the ability to share information with external organisations.

These two points define a clear weakness in the current information security domain, and underpin a research agenda to investigate the problem of content-based access control to information shared outside of an information system perimeter.

The Jericho Forum, a working group of information security officers/architects from some very large organisations such as Boeing, HSBC, and the pharmaceutical company AstraZenica, has also identified these weaknesses and has coined the term de-perimeterization (De-P) to describe it [Jer07]. De-P is the realisation that information system perimeters are becoming less effective due to the expanding boundaries of organisational network perimeters in support of collaborative working. They believe the expansion will reach a point, where information would be better protected if the perimeters were no longer

used as the access control point between the outside world and the information. Instead, information should be controlled at the content level and be able to have policy enforced wherever it resides. They do not provide solutions, but have written several position papers on this subject, indicating the same security requirements are evident in large corporate environments [Jer08], and that the IT industry is not currently providing a solution to them.

Microsoft has also recognised that network perimeter security is becoming a dated approach. In a keynote speech at the 2007 RSA conference [Mur07], Bill Gates and Craig Mundie commented on the requirement for more flexibility in control of networked resources. To quote Mundie, “We could continue to invest in this fortress mentality of protecting everything, but I don't think that will be sufficient”, this suggests that Microsoft are thinking along the same lines as the Jericho Forum in recognising that securing a perimeter around the resources of an organisation is not the answer to all information security problems. He continued, “most people would agree that our castle is fairly porous, because a lot of the assets actually leave the castle”, this relates to the problem of controlling information resources outside the network perimeter. It supports the argument for the ability to enforce access control policy remotely and to be able to modify access control policy for centrally managed distributed information, in the modern electronic information world. It is also impossible to assume the secure perimeter is impenetrable. Even if it was, to enable collaborative working, collaborating partners need to allow their perimeters to be breached to some degree and information to be moved from system to system in order to support collaboration.

2.3. Threat Model

2.3.1. Risk Assessment

The literature review of current issues and approaches to electronic information sharing and management uncovered many situations where sharing information in distributed collaborative environments puts the information at risk. The risk to information in any given situation is determined by conducting a risk assessment. Many risk assessment methods take a quantitative approach to risk, which defines a set of assets to be protected, potential vulnerabilities of the assets, and the likelihood of a threat agent exploiting the vulnerabilities [ISO05, Cob06]. The likelihood of a threat agent exploiting a vulnerability, and the impact of this on the organisation, usually financial, are two indicators that are often ranked on a

numerical scale and multiplied together to make a total risk factor, i.e. the likelihood of a threat agent exploiting a vulnerability, multiplied by the impact of this happening, gives the total risk factor. Because the information sharing scenarios discussed in this chapter are largely focussed on unquantifiable risk, as they are not focussed on the financial impact of risk; a qualitative approach is taken to risk assessment here. This involves drawing out the most pertinent risks to information from the situations found in the literature review. Government reports and legislation have a reasonably large impact on this, due to modification of data protection laws and the fact that information owners will soon be liable to civil action for not providing appropriate security for their information. In the light of the emerging use of information sharing in collaborative distributed environments, the threats highlighted in these reports are particularly relevant.

The risks identified in the qualitative risk assessment, form the basis of a system threat model. Threats, in this model, are defined as situations that exist in the information sharing environment where the information is at risk. It is possible to classify threats into three categories:

- Anticipated threats where it is not deemed necessary to mitigate
- Anticipated threats that can be mitigated
- Anticipated threats that cannot currently be mitigated

All possible anticipated threats to information shared in a collaborative distributed environment make up a complete *threat model* for that environment. To develop a security focussed solution which reduces or mitigates some of the unmitigated risks posed by threats to information in such environments, it is possible to select a subset of the full threat model and create what will be known as a *system threat model*. The system threat model, effectively a requirements definition, contains mostly unmitigated threats from the information sharing environment. The system threat model will be used to inform the enhancement of the basic access control framework from Chapter 1, by identifying where the gaps in security provision currently lie. It will also be used to evaluate the prototype technology used to test the feasibility of implementing the new framework, on completion of the research, to determine to what extent the technology protects information against the unmitigated threats identified.

2.3.2. System Threat Model

Taking a qualitative view of risk to information shared in distributed collaborative environments, the situations outlined in this chapter contribute to a three tier system threat model that drives the development of the approach to access control documented in this thesis:

The main risk to information shared in collaborative working environments is unauthorised access and use of information. This threat arises because of the current approach to controlling access (see Chapter 4), by using perimeter controls. The approach does not scale to enable security in distributed collaborative environments, as is evident from the documented data losses, and the HMRC and CPS clamp down on storing sensitive information on removable media and taking it outside of the perimeter. This means that any information shared outside an organisation's network perimeter can no longer be protected using the original perimeterized access control mechanisms.

A secondary level of risk is the lack of sustained, modifiable control over shared, distributed information. This threat to information occurs because, if access was granted initially to a collaborator, there is no means of revoking access to that information, if required. There may be several situations where revoking access may be necessary. For example:

- The collaborator may prove to be untrustworthy, if it is reported that they have had their systems hacked or lost portable media where sensitive information has been exposed;
- The collaboration relationship may come to a scheduled end and the owner of the shared information may wish to retain intellectual property rights, and therefore revoke further access to that information;
- Previously shared information becomes reclassified, so that it is unsuitable for sharing.

A further level of risk is the lack of granular control over content within shared resources. When information resources are shared between multiple organisations, the access control rights granted to each organisation by the resource owner may vary. As the Data Handling Procedure in a UK Government report by the cabinet office [HMG08b] states; some information requires a greater degree of protection than others. Going back to the healthcare

scenario, a patient's medical history may be shared from an electronic health record, while their current medication and long term illness status may be restricted to only some of the collaborators. The threat to content comes when it is merged into a single resource, which is given a single security label. While it is desirable to share the patient record, the resource owner cannot separate control of the restricted content from the rest of the resource, making it very difficult to do so. The ongoing effort to achieve acceptance of the Electronic Patient Record (EPR) in accordance with the British Medical Association (BMA) Security Policy [And08] exemplifies this. More people now have electronic access to patient information and current efforts have not managed to implement an effective means of "sealing and locking" parts of the patient record to provide selective restricted access while allowing freer access to other parts.

Chapter 3 - Access Control Models

Several major access control models exist that aim to provide approaches to restricting access to information, based on rules and relationships. These models are either multi-level security models, based on a hierarchy; or multi-lateral models, based on information flow. This chapter investigates both the multi-level and multi-lateral models and places them within the framework introduced in Chapter 1.

For reference, part of the basic access control framework is repeated below.

Let D be a set of documents.

Let C be set of information classification schemes.

Let U be a set of users.

Let A be a set of actions (to be performed on a document).

Let R be a set of access control rules.

This basic access control framework will be used to analyse existing access control models and derive ways of representing the rules and relationship required to link the security labels of users and documents, to a rule set that determines whether access should be allowed or denied.

3.1. Multi-Level Security Models

In a multi-level access control model we would expect to see a hierarchical classification scheme being used to assign a security level to users and documents. An example of a hierarchical classification scheme is the military and governmental classification scheme of *Unclassified*, *Classified*, *Secret*, *Top Secret*. These levels are used to derive the access control rules. For example, the Bell-La Padula access control model [Bel05], which is a multi-level model, defines a set of classifications based on the hierarchical military classification model (top secret, secret, classified, unclassified), and a list of categories related to the domain of the information (e.g. home affairs, foreign affairs). Levels of restriction to information are defined by assigning each information resource one classification label and one or more

categories from the list. In addition, each user is granted a classification label indicating the highest level of classified information they can access, and one or more category labels – information domains to which they have access. The model defines two access control rules for use with the classification labels:

- Simple security – dealing with reading information.
- The star or * property – dealing with writing information and creating new information.

The simple security rule deals with read access and states that a user (u_z where $u_z \in U$) may only access a resource (d_x where $d_x \in D$) if their classification label (c_{ku} where $c_{ku} \in c_k \in C$) is equal to or higher than the label of the resource (c_{kd} where $c_{kd} \in c_k \in C$). Thus to read a document $c_{ku} \geq c_{kd}$ must be true. This prevents people from reading information above their label, sometimes referred to as “no read up”. This means that if $c_{ku} = \text{‘Secret’}$, and if the user tries to read document d_x where $c_{kd} = \text{‘Top Secret’}$, the request will be denied because their classification label is below the classification label of the information.

The star or * property defines write access rules and states that a user (u_z) may only write to a resource (d_x) that has a classification label higher than or equal to that of the user. Thus to write to a document $c_{ku} \leq c_{kd}$ must be true. Taking the example used in simple security, this means that if $c_{ku} = \text{‘Secret’}$, the user can write to d_x where $c_{kd} = \text{‘Secret’}$ or ‘Top Secret’ , but cannot write to the lower classified information. This rule is often referred to as “no write down”. The Bell-La Padula model aims to preserve information confidentiality by preventing users from reading information classified above their level and writing higher classified information into lower classified documents, thereby exposing the content to those with lower security levels.

While the Bell-La Padula model attempts to assure confidentiality, the Biba multi-level model [Bib77] was developed to provide integrity. Bell-La Padula restricts users to “no read up, no write down”, but an issue arising from the star property is that users are able to write to information that is above their level, meaning that if $c_{ku} = \text{‘Secret’}$, the user (u_z) could, in theory, write information to a document (d_x) where $c_{kd} = \text{‘Top Secret’}$, which they are not even allowed to read. In an extreme case, this gives the user the potential to overwrite all of the information in the document so it no longer contains any information or inaccurate information. The Biba model was developed to support the Bell-La Padula model. Its aim is to ensure that users cannot change information content above their own classification label so

that it is no longer accurate, or becomes corrupt. Biba has the same two rules as Bell-La Padula – Simple security deals with reading, and the star or * property deals with writing. The difference is that both rules are the opposite of Bell-La Padula. That is, “no read down, no write up”. Instead of simple security stating that a user is not able to read information above their classification label, the rule restricts read access to information that is *below* their label, formulated as $c_{ku} \leq c_{kd}$. The star property switches from restricting write access to information below a user classification label to stating that a user cannot write to information above their label in the Biba model, formulated as $c_{ku} \geq c_{kd}$. The opposite of the Bell-La Padula rules. The majority of the time it is relatively harmless to allow a user to read information below their classification level, but it is imperative to ensure that users cannot write to information above their classification label in order to maintain the integrity of the information.

The Bell La Padula and Biba models combined equate to $c_{ku} = c_{kd}$ which is the model most organisations use when protecting their information. This rule means that a user, given a security level, can only read from and write to documents with the same security level as their own. While currently, labels are typically applied to entire resources, the work of Bell-La Padula and Biba has created a means to classify different sections of content within a resource at different levels, and map access rights to those sections to user classification labels.

Denning’s Lattice model is another multi-level approach [Den97], which focuses on the secure flow of information within a system. The principal is that information can only flow between users if the recipient user’s classification label is equal to or higher than the sender’s. For example, User Z, where $u_z c_{ku} = \text{‘Secret’}$, can only send a document to user Y, if $u_y c_{ku} = \text{‘Secret’}$ or higher, formulated as $u_z c_{ku} \leq u_y c_{ku}$, effectively equating to the Bell-La Padula star property.

Denning’s lattice brings out one of the major problems with both multi-level and multi-lateral approaches, indeed with the basic access control framework in general. That is, in order to accurately enforce controls using conditional rules, the classification scheme used to label information must be based on a common scheme for all documents. This is feasible for a single organisation but much more complex in a VO environment, where each organisation in the VO may have a different interpretation of what each classification scheme actually means. If User Z and User Y are from different organisations, the problem of how to convey

and resolve differences in the meaning of classification labels between the organisations becomes an important issue when perimeter secured information is shared outside the perimeter.

Given that access control decisions in multi-level access control models are made by mapping a user's security label to a document's security label through a hierarchical rule, using elements from the basic access control framework, we can define a formula that can be used to represent all possible hierarchical access control rules, $r_a = c_{ku} + \{=, >, <, >, <\} + c_{kd}$, which we can call the **basic access control formula**. We can say this formula is able to support hierarchical access control decision-making as long as the classification scheme c_k , from which the labels are selected, is supported by all systems that intend to implement the formula, so that the labels have the same meaning. This means that c_k must either be the same between the systems, or there must exist some mapping between c_k and the classification scheme of other systems. For example $c_k = \{1,2,3\}$ of the system used by User Z could map to $c_l = \{x,y,z\}$ of the system used by User Y where $1=x$, $2=y$ and $3=z$. So, if $u_z c_{ku} = x$ and $u_y c_{lu} = 1$, even though different classification schemes are used (c_k and c_l), the meaning of the label is the same between systems. The same applies to document labels. Problems with enforcing access control across set boundaries begin to occur when different classification schemes have ambiguous interpretations or mappings. In a multi-level model this may occur where the security level in one scheme only maps partially to a level in another. Another problem is the sharing of rules. Just because the labels have the same meaning does not mean that the security manager of system Z is satisfied for User Y of system Y to gain access to their documents, even though the labels used to classify documents within system Z can be mapped to those used in system Y, and user Y has the appropriate label for access within their own organisation. This is part of the problem of perimeterized access control, as defined in Chapter 1, and will be discussed further in Chapter 4.

Landwehr's military message access control model [LHM84] identifies that an information resource – in Landwehr's case a military message, may comprise component sections of content with varying security levels. For example, the message may contain a number of paragraphs; each assigned its own security level. This principal is very relevant to this research. Landwehr introduces the concept of a *container*, an information resource with a multi-level classification scheme that may contain other containers, each with their own classification. This model really addresses the concept of finer levels of granularity within a restricted information resource. It exemplifies the potential strength of the Bell-La Padula and

Biba models for enforcing confidentiality and integrity. However, Bell and La Padula also realised that one cannot protect resources with finer granularity than the protection mechanisms themselves support. Thus, the current approach of controlling access to entire resources as a single entity, prevents access control models such as Landwehr's model from becoming implemented in electronic access control environments and providing more refined, granular levels of control.

3.2. Multi-lateral Security Models

Multi-level security models are not necessarily the natural choice for information sharing in modern VO environments. Both Bell-La Padula and Biba models of access control stem from military security requirements, where the focus is on preventing the downward flow or upward modification of information through a hierarchy. In modern VO environments the flow of information may be more laterally controlled with the information being prevented from flowing “across” organisational domains. This type of control is known as multi-lateral security. In a multi-lateral security model, the security considerations are slightly different. There is no hierarchical classification scheme to assign security levels. Rather, the focus is on information flow.

An example of a multi-lateral model is the Chinese Wall model [BN89] which considers professional competition logic to restrict information flow between users who have roles with a conflict of interest, such as the corporate advisory and investment roles within investment banks, and the editorial and advertisement roles within a newspaper. The rule is that if an individual has worked or is currently working for an organisation in a particular sector, they are not able to share information with another organisation in the same sector.

Another model that focuses on information flow is the Clark-Wilson model. Clark and Wilson published their concerns regarding the focus of the Bell-La Padula model and other so called lattice based approaches on a military requirement for information security, and how this does not necessarily map onto commercial requirements [CW87]. A lattice based model generally describes any approach to access control involving multiple users and targets (information resources), where a conceptual lattice structure is formed through the definition of relationships between the security labels of users and targets, as formulated within the basic access control formula in Section 3.1. They argue that there are two distinct classes of access control mechanism required, as they believe that security policies and mechanisms

required in commercial environments are very different to that of the military. Their stance is that the model used in the military based approach, as proposed by Bell-La Padula, is too simplistic to solve the entire problem of commercial information restriction. Their suggestion is that a well formed transaction, and separation of duties among employees, is needed.

The well formed transaction relates to logging and audit, where user actions can be traced at a later date to check for unauthorised data modifications or actions. This works by firstly making the user aware that their actions are traceable to deter them from malicious activity, and providing an audit trail to determine the malicious user if such activity occurs. In the case of information sharing in VOs, this could potentially relate to an audit history of access control and information sharing, i.e. who had access to specific information, and between which dates and times were they granted access. This information would be used together with details of information breach or misuse i.e. specific information content, date and time of the breach or misuse, to build a case and determine who was responsible for the data breach or misuse in a court of law.

Separation of duties involves separation of business processes into subparts that are executed by different people. For example, the process of purchasing an item involves several steps: authorising a purchase order, recording the arrival of the item, recording the arrival of the invoice and making payment. The next task in the process should not proceed unless the previous task has completed correctly, and each task should be performed by a different person. Collusion aside, this is a very effective method of preventing fraudulent activity. Clark and Wilson's suggestion to separate duties is that it is necessary for a computer system used for commercial data processing to ensure that a data item can only be manipulated by a certain set of programs that have been inspected for proper construction, and controls must be provided for the capability to install and modify these programs. This provides a level of integrity in the programs that are operating the business processes. To ensure separation of duties, each user should be permitted usage rights to a specific set of programs based on the requirement to use those programs as part of their duties as an employee. The major difference between the Clark-Wilson model and Bell-La Padula models is that there are no multi-level security attributes assigned to users and targets within the system; rather a specific set of applications allowed to manipulate a resource is defined, together with a set of user constraints on the use of those applications to read and write information. The user is not restricted on the information they can read and write, but on which applications they can execute. There are implicit information access and modification restrictions applied to these

applications. Both the Bell-La Padula and Clark-Wilson models have an underlying concept of mandatory access control. Bell-La Padula requires the classification of users and targets with security labels, and a supporting architecture to enforce these rules. This relates to the basic access control formula. Clark-Wilson puts the control over user actions with the applications on the system itself, and classifies a user by granting access to specific applications. Furthermore, controls that may be considered in a multi-lateral model may consider geographical borders where legislation and regulation may not support the level of security required, and to a certain extent, temporal constraints such as limiting access to information between the hours of 0800 and 1800. To contextualise multi-lateral access control in the basic access control framework, we must allow an information classification scheme, c_k to be considered as more than a hierarchical and structured scheme, and consider it as a tuple of information flow restricting requirements, such as role, domain, geography, time, and of course there is no reason why levels from a multi-level classification scheme cannot be added to the tuple. For example, in addition to $c_k = \{x,y,z\}$, $c_k = \langle \{x,y,z\}, \{user,admin,guest\}, \{europe,asia,north_america\} \rangle$, where $c_{kd} = \{x,admin,europe\}$. This means the user's label must represent the ability access level 'x', have an 'admin' role and be accessing the data from within 'europe'. The important point to note from the access control framework point of view is that the basic access control formula that maps a user's security label c_{ku} against a document's security label c_{kd} , when evaluating whether to allow or deny access to a document, still applies in a multi-lateral model, albeit with additional labels. The problems of different classification schemes having ambiguous interpretations or mappings could still occur in multi-lateral models. Indeed, in a multi-lateral model it is possible that the problem will be exacerbated due to the complexity of security tuples including controls based on geography, roles and time.

3.3. Desirable Features of an Access Control Model for Collaborative Distributed Working

In conclusion, the desirable features to be supported in an access control framework, with the aim of improving information security in collaborative, distributed VOs would be the ability to:

- Classify users and assign labels based on the levels of access they are allowed, in order to define the maximum level of information a user can access. This is based on the strengths of the Bell-La Padula and Biba models. It limits user access to information, when access is not required to carry out their tasks in an organisation.
- Classify content within information resources to a much finer-grained level, in line with the Landwehr model for access control. This allows content with varying levels of sensitivity to be classified at different levels in the same resource, and also allows contributors to an information resource to classify their own information, with their own protection requirements.
- Support classification label interoperability between organisations, so that classifications defined by one organisation can be interpreted by another organisation when accessing and handling information. This is an issue from studying the application of Denning's lattice, in collaborative environments, between multiple organisations.
- Be implementable as machine enforceable controls, so that classification labels can be related to access control restrictions, and controls can be enforced. This would enable mandatory access control through a software infrastructure, as suggested by Clark and Wilson's separation of duties model.
- Support an audit trail by logging user access requests, as suggested by Clark and Wilson's well-formed transaction model. In the case of information misuse, an audit can be performed to analyse actions which determine the acting parties.
- Ensure that information is not released to collaborating organisations that have a conflict of interest, based on the Chinese Wall model.

These desirable features have been defined from the literature review of existing access control models. They will be used in the next Chapter to analyse and compare the functionality of existing access control technology, which are effectively implementations of access control models, and identify shortcomings in existing access control technology when evaluated against the set of desirable access control model features in this section, the System Threat Model defined in Section 2.4.2, and the limitations of the basic access control framework identified in Section 3.2. The analysis will draw out how existing implementations of technology implement the basic access control framework, and abstract

additional framework elements with the aim of defining a framework to support the hypothesis.

Chapter 4 - Existing Access Control Technology

The problem of maintaining fine-grained control of information outside the perimeter was highlighted in Chapter 2. The desirable features of an access control model for collaborative distributed working were defined in Chapter 3. This chapter investigates the limitations of current access control technology in dealing with the problem of maintaining fine-grained control of information outside the perimeter, and how they implement access control models to enforce access control.

4.1. Access Control Techniques

To control access to restricted resources there are two archetypal methods used: Authentication and Authorisation [ISO96]. Authentication is the process of requesting some identity credentials from an entity that is attempting to access a resource, and consequently determining whether the entity is indeed who they portray to be. Once authentication has taken place, Authorisation is used to grant access rights to an entity and limit the accessibility and actions that can be performed on the resource. This is based on the identity credentials of the entity, using a pre-defined access control policy. Access Control systems associate three major components with its use; *subjects* – users, services and other entities that intend to access and possibly manipulate information; *targets* – the information involved in the subject's access request, and *rules* – these define the subject's access rights to the target. These three components form what is known as an Access Control Policy.

There are two general methods for enforcing access control: discretionary access control (DAC) and mandatory access control (MAC). DAC is based on a human decision about the access and usage rights granted to each subject, in relation to whether a subject should be allowed to access a particular target. This is a very subjective means of applying access control. In a VO environment, the management of user privileges is quite often managed by the VO as a unit. A nominated group of members or perhaps all members of the VO carry joint responsibility for controlling access to the information resources used within the VO, which will often include resources from several organisations. Because of the human intervention aspect, DAC may not be the type of control that information security administrators of restricted information within a VO would be confident of relying on, as an administrator would be subjecting information to the discretionary control of other members

of the VO. In the real world this could relate to allowing collaborating business partners to have an opinion and some control over how an organisation's information is shared, and to what level it is protected, with an uncertainty as to what might happen to it or how it might be exploited. For information protected under the Data Protection Act (1998), and sensitive military or commercial information, this could, and should, be unacceptable to information owners, because of the liability faced by the individuals responsible for its protection. DAC may be an approach used by VO members to define an access control policy for information within their own system, because they are in control of this information, but for distributed electronic environments, resource owners require a more rigid and consistent enforcement of access control.

MAC offers a more rigid and consistent level of control, in which the computer system enforces the access control based on a set of pre-defined rules. MAC is based on security labels, where each subject in the system is given a label reflecting its level of responsibility and access rights, and each target is also given a label that specifies the level of rights required to access it. This is a technical interpretation of multi-level security, as illustrated in Chapter 3 with the Bell-La Padula and Biba models. When a subject attempts to access a target resource, the system determines whether access should be allowed, based on a comparison of the subject's security label and the target's security label. A conditional set of rules state how the two should relate, with the Bell-La Padula and Biba models defining that access should only be granted if the subject's security label is equal to that of the target. Chapters 1 and 3 formulated this using elements from the basic access control framework, as the basic access control formula $r_a = c_{ku} + \{=, >=, <=, >, <\} + c_{kd}$. One issue with MAC is that a subject may have multiple roles within an organisation, with different associated security labels. In a VO environment this means that a user may have multiple identities within a VO with different associated security labels. For example, a user may be the administrator of the VO, and thus have full access to the access control policy for the VO, but also be a member of the VO and have limited access to restricted information shared by a collaborating organisation. The organisation sharing the restricted information within a VO has to trust the user to log into the VO using the member account, when accessing information and not change level of access rights by using the administrator account. This is where the Clark-Wilson model of separating duties and recording transactions becomes important. The logging of information access and modification makes it possible to audit the use of roles in accessing information, and monitor activity within VOs.

Assuming some level of mandatory access controls are required within an information system, there needs to be some method of electronically creating and storing the rules represented using the basic access control formula, that define who the subjects are within a system and what access privileges they should be granted to the target resources on the system. Typically this has been provided by a list of rules known as Access Control Lists (ACLs) [SS94]. Operating System access controls use ACLs for access control and they are common within organisations to provide a means of identifying access rights of users within an information system. ACLs are essentially a list of rules stored in a file that stores some piece of identifying information about a subject, usually a username, and for each target on the system, an explicit rule as to whether the subject is allowed or denied access. In some cases this may be extended to action controls (read/write/execute) for the target. Using elements from the basic access control framework, we can express mandatory access control decisions as a function $f(u_z, d_x, a_i, r_o)$ where, as illustrated in Figure 4.1, a MAC system works by passing a user identifier (u_z) together with the target document identifier (d_x), a requested action a_i , and a set of rules (r_o) to the function. The function then determines if the requested *action* is allowed or denied by evaluating the set of rules (r_o), which is stored in the ACL, and a result of ‘allow’ or ‘deny’ would be returned. The function can include labels, but they are not usually considered within ACLs.

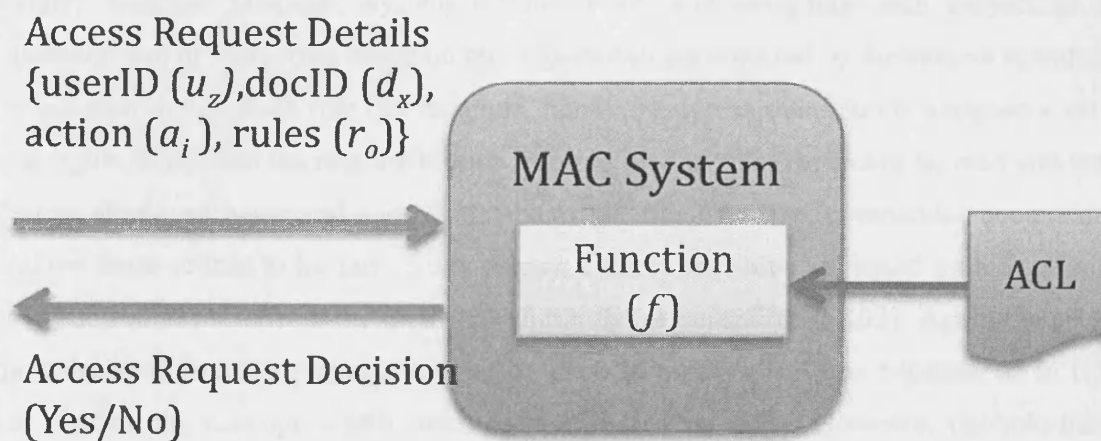


Figure 4.1 – The Mandatory Access Control Approach

The desire to create an access control policy that allows system administrators to assign access rights to subjects of the system, based on a flexible and discretionary set of rules, gave rise to the concept of Rule-Based Access Control [LZXQ05]. Rule-Based controls involve setting up fine-grained parameters by which an individual can access resources on a system.

As the name suggests, these parameters are written as rules such as “user X can access resource Y, but cannot access resource Z”. This can be also represented using the access control decision function $f(u_z, d_x, a_i, r_o)$. However, in this case, an ACL is not used, rather a rule base is accessed to determine the result. In Figure 4.1, the ACL would be replaced by a more detailed set of rules. This concept, although a major step forward towards the realisation of flexibility requirements, causes a complex scenario for administrators of large systems with hundreds of users and thousands of resources. The maintenance of a list of rules for a system of this size would be very time intensive and thus not easily scalable or maintainable. In a VO environment where users have a dynamic presence and role within the VO, they have varying levels of responsibility and access rights, making rule based controls of this nature very unfit for purpose, due to the amount of human effort and time required to maintain the rules. Users enter and leave VOs at a much more rapid rate than conventional organisations meaning that the lists have to be kept up to date after each change in VO membership. As a concept, Rule-Based access control is not suited to dynamic or large-scale environments, and this flaw is one reason why Role-Based Access Control was developed.

Unlike *Rule-Based* Controls where each subject is assigned a set of rules to control their access rights, *Role-Based Access Control* (RBAC) [FK92, SCFY96] is based on the real-world organisational concept of developing a set of roles within an organisation: e.g. Manager, Assistant Manager, System Administrator, and assigning each subject in the organisation one or more roles based on the responsibilities required by the subject in order to carry out their duties. Each role (for example, human resources manager) is assigned a set of access rights that reflect the responsibilities required by that role (for example, read and write access to employee name and address database, salaries database, contractual documents), and allow those actions to be carried out. Access control decisions are based on the actions a user is allowed to perform under their role within the organisation [FK92]. Again the access control decision function $f(u_z, d_x, a_i, r_o)$ can be used to make decisions because, as in rule-based control, the concept is still fundamentally based on rules. However, the role-based approach is much easier to maintain, as there are fewer roles than employees within the organisation, which means it is easier to the access rights. For example, if an organisation has five hundred employees, in a rule-based list that would mean managing and maintaining five hundred lists, whereas in a role-based approach the organisation may have fifteen roles for those five hundred employees, meaning only fifteen access control lists are needed and a correlating employee(u_z)-role table. If an employee’s role changes, in a rule-based

environment there could be several changes required to access control lists, and this would be almost impossible to keep track of in a dynamically evolving VO, where it would be common for members to change roles frequently. Whereas, in a role-based control environment, the administrator can simply change the user's role to one that encompasses all the access right rules of their new position, and the change of access control takes effect immediately the next time the user logs in. From a scalability and dynamically manageable point of view this functionality is imperative and makes role-based access control very suitable for VO environments. This is where an information classification scheme and labels can be useful. Instead of complex rules or an explicit rule for each user-resource relationship, users can be given a security label from an information classification scheme, as can resources, and rules can be set that define the relationship required for users to access resources, as formulated in the basic access control formula $r_a = c_{ku} + \{=, >=, <=, >, <\} + c_{kd}$. If a person changes their role, they change their label. Resources remain at the same level of classification; users change the levels of classification. The rules defining who can access what are stored in an ACL-like document, based on the basic access control formula. The access control system, as illustrated in Figure 4.1 still applies, but with the addition of a classification scheme, as shown in Figure 4.2. With the addition of labels in addition to and document identifier, the access control function becomes $f(c_{ku}, c_{kd}, a_i, r_o)$, where the user and document identifiers are replaced with security labels.

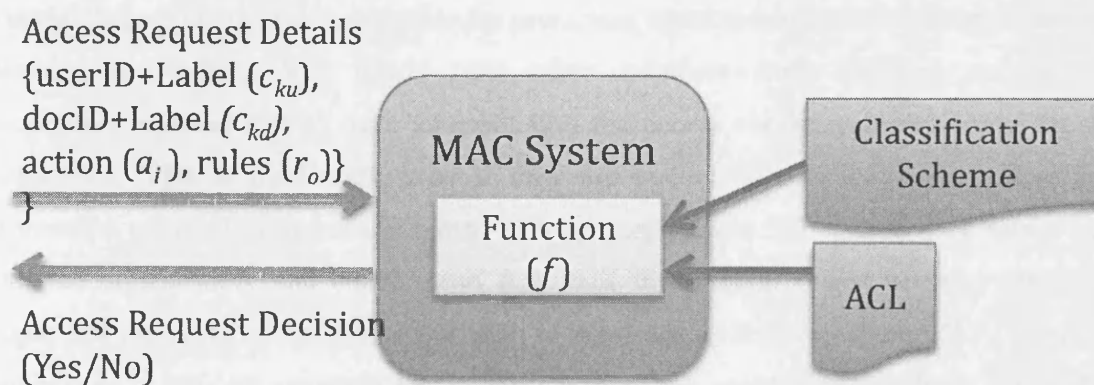


Figure 4.2 – MAC System for RBAC

As role-based control is MAC based, there is still the problem of managing multiple roles for subjects. A user could have multiple roles encompassing different levels of access control. Where subjects hold multiple roles, there is still a requirement to trust them to use the appropriate role for their current duties and not just use the highest level role to carry out all

tasks. In a VO there may be frequent changes to a subject's role, and new roles may be created dynamically for specific tasks within the VO. Thus, the administration of access control policy is an important issue in such environments.

4.2. Access Control Administration

If an Access Control Policy is centrally controlled, a single authority is responsible for the derivation, maintenance and enforcement of the policy and its rules. In a VO environment that is configured to be centrally managed, this means members from disparate organisations managing the access control for the entire VO from a centralised point. One concern that could arise in a centralised approach is the potential for a bottleneck when large numbers of system users are requesting the service from the system, to authenticate and authorise them at the same time. At busy times of the day, such as first thing in the morning or after lunch, this could have a significant impact on the performance of the system. Another concern is that a single point of access also means a single point of failure. If the access point is unavailable for whatever reason then nobody can get authorisation to access anything. A way round these problems is to have mirrors or backups of the access control system that become available, if the access point becomes unavailable, to replace the failed access point. However, another concern, which is in fact one of the most important issues with this approach within a VO environment, is how to define and enforce community policies [PWF+02]. It is highly doubtful that a VO member responsible for protecting restricted information being shared in a collaborative working VO, would trust other members from different and possibly competitive organisations to have an input into the access control rule definition for their information. This is particularly true if they are responsible for personally identifiable information under Data Protection Laws. This approach takes full control over access away from the organisation, and could mean that their information might become exposed to people that the organisation would not wish to grant access to, even though they are fellow members of a VO. An approach that solves some of the centralised problems, particularly those identified above, is decentralised control. In decentralised access control [SCK+06], each organisation manages its own access control point that manages the rules protecting its own resources. This puts the onus on the organisation to protect its own information, as if anybody gains unauthorised access to any of its resources, the cause is them not maintaining a proper set of access controls. While reducing the amount of trust required in the VO management to protect resources, the decentralised approach assumes that the resource itself

is physically stored within the secured perimeter of its owner's system. This is one area where current decentralised approaches fail to support secure collaborative working. It is also where the need for de-perimeterization becomes evident. The traditional method of securing information, as used in the centralised and de-centralised approaches, is to store documents in protected perimeters and enforce access control at or within the perimeter. Network perimeters are the most commonly used barrier between users and documents, as described in Section 1.2. However, a distributed collaborative information-sharing environment is inherently detrimental to the security of information secured using this approach, because to share information the documents often have to leave organizational perimeters, rendering the access control technology used to protect the documents ineffective, no matter whether the administration is centralised or de-centralised. For example, if a GP e-mails a patient record to a clinical consultant at a hospital, or gives them access to an online repository from which the record can be downloaded, the document that comprises the record moves from within the GP's perimeter to the hospital's perimeter where the controls used to restrict access within the GP's perimeter cannot be used to enforce access control rules. The real requirement, as hypothesised in this research, is to enable more effective information sharing by supporting the enforcement of rules defining an information resource's access control, wherever the information is stored or used in an Internet connected environment, rather than the current perimeterized approach where the information resource must remain under the control of its owner to enforce access control. If this were possible, then the trust requirement from a resource owner point of view would be shifted from allowing somebody else to manage and control access to its resources, to the ability to be able to trust that the access control enforcement technology can accurately perform authentication and authorisation of a subject, a model suggested by Clark and Wilson. Resource owners would remain in control of their information, by managing a local access control policy, while the policy itself could be enforced on information that has already been shared. The information would *not* have to remain under the control of its owner to enforce policy.

This discussion is introducing a new element for consideration in addition to the existing basic access control framework. This is enforcement control. Enforcement controls are absent from the basic access control framework because so far the investigation has focussed on existing access control models, that is, how to model access control *decisions*. Enforcement is independent of access control model. Indeed, it is an implementation of the result of a decision made using an access control model. To address this issue, the study focus will now

move to the implementation of access control model decisions and investigate the technology that is used to enforce access control.

4.3. Access Control Technologies

This section first provides an overview of some of the supporting technologies used within security architectures to enforce confidentiality and integrity in distributed systems, and continues with a literature review of the most prominent and related technology implementations currently published.

4.3.1. Confidentiality, Integrity and Identity in Distributed Systems

4.3.1.1. Achieving Confidentiality

When sending information across unsecured networks such as the Internet, where snooping third parties may intercept the information and use it for their own purposes, it is important that the information is protected while in transit, so as to maintain the confidentiality and integrity of the information. Confidentiality in this sense means that *only authorized people can read the information*. The most commonly used approach to protecting information while in transit is cryptography, an approach that provides confidentiality through the transformation of plain text into a form that is unreadable to humans called cipher text using an encryption algorithm and an encryption key. Applying cryptographic techniques to an information resource means that anyone who intercepts the information cannot use it to their advantage, as it is meaningless to them, unless they know the algorithm needed to decrypt it, and possess the encryption key to reverse the transformation and decrypt the information. The algorithm is normally made public as they do not need to be kept secret, and there are a number of encryption algorithms that are in common use within organisations and within messaging clients such as email applications. The important component to be kept secret is the encryption key, as this is the component that keeps the encrypted information “locked”. Each party that wishes to decrypt the information must have prior knowledge of the algorithm to perform decryption, and the encryption key, as this is applied to the information. This approach is known as Symmetric Cryptography since the sender and receiver must use the same key to encrypt and decrypt messages. Symmetric Cryptography has some important flaws in its provision of information security, namely:

- How to send the shared key to all relevant parties. Any snooping third parties that might intercept the information that is to be protected might also intercept the shared key if it is sent across the same unsecured channels, in which case they can use it to decipher any encrypted messages they intercept in the future that use this key.
- Once the shared key is given out by the sender there is no control over what information the other parties can decrypt with that key. For example anybody could use the same key to decrypt other information that the sender has encrypted using the same key including future messages the sender might transmit that are not meant for the eyes of previous receivers. Thus, it could be used to access files on the sender's local machine that have been encrypted.

To overcome these flaws, the concept of Asymmetric Cryptography was introduced. In this technique, senders and receivers of information do not share a single key for encryption and decryption; instead they each have a pair of keys known as public and private keys or the key pair, hence the reason for asymmetric mode often being known as Public Key Cryptography. These keys work in such a way that information encrypted using the public key can only be decrypted with the corresponding private key and vice versa. A passphrase known only to the owner of the private key prevents the private key from being used without entering the correct passphrase for the key when attempting to use it for encryption or decryption. A passphrase is similar to a password but is more complex as it can include many symbols and characters and is typically much longer than a password making it more difficult to hack or guess. The underlying concept is that the public key can be made available to anyone by sending it via email, on a memory stick, or storing it in a networked directory, essentially it does not matter who has possession of the public key, so it can be sent across unsecured channels. A person can then use a public key to encrypt information and send it to the person who they believe to be the owner of that public key, confident in the knowledge that the only person who can decrypt the information is the person with the corresponding private key and passphrase. If the information is intercepted, it is not a problem, as it cannot be decrypted without the private key or passphrase. If the information is sent to the wrong person, i.e. not the owner of the public key used to encrypt it, it is an inconvenience but still not a problem, as only the owner with the corresponding private key can decrypt it. The major difference between the symmetric and asymmetric methods is that the private key is not required to be shared and indeed should never leave the possession of its owner. The private key can be resident on a local machine, laptop, secure token or whatever storage medium the owner

chooses, but careful control of it must be exercised as, along with the passphrase, it is the “locking” and “unlocking” secret for encrypted information. Further, when the private key is used to decrypt the information, the person will be prompted for the passphrase which protects the private key usage, meaning that if the person has the private key but not the passphrase to use it, encryption or decryption cannot occur.

4.3.1.2. Achieving Integrity

Confidentiality through encryption is only one of the purposes of public key cryptography. The encryption of information using a public key ensures that only the individual with the corresponding private key can decrypt it. Conversely, the private key can be used to apply what is known as a Digital Signature to an information resource. Digital signatures involve the encryption of an information resource with an individual’s private key. The only way to decrypt information that has been encrypted with a private key is to use the corresponding public key. Of course, this may be obtained by anybody, which means confidentiality using this approach would be minimal; however, confidentiality is not the aim of digital signature. The private key cannot be utilised unless a person has prior knowledge of the passphrase required to use it. This adds integrity to the information encrypted with a private key, as anybody decrypting the information using a public key knows that the information almost certainly will have originated from the owner of that public key and nobody else. Integrity in this sense means that *information is only modified by those authorised to do so*. Using public key cryptography in this way is one method for providing user authentication. Electronic messages such as requests for access and shared information can be signed with digital signatures and will carry the identity stamp of the user sending the message. This approach allows access control infrastructures to automatically pass identity attributes between distributed access control systems without the user having to provide a username and password each time they interact. In addition to the authenticity of the information, digital signature also means that upon decryption of information, the person reading it can be sure that the information has not been tampered with or modified at all since its encryption by the person who generated the information. This technique is often used in email to prove that the email originator was indeed, who they portray to be and it is not a spoofed email from an impostor. This provides confidence in the integrity of the email, as it will not have been modified since it was sent, as there is no way anybody else could have encrypted it with a private key unless they used the originator’s private key.

4.3.1.3. Achieving Confidence in Identity

Public Key Encryption also allows user identity to be passed between electronic access control systems automatically, and it supports user authentication on actions such as requests to access information. However, like other forms of identity token, a public key is susceptible to imitation by fraudulent people pretending to pass a public key with a fraudulent identity as their own. The success of public key cryptography depends on the establishment of trust in a public key, that it does in fact belong to the person that is presenting it as their own, and that the person is who they claim to be. This requires an ability to unquestionably bind public keys to the identity of a person. These requirements are addressed by the Public Key Infrastructure (PKI) framework [BFPW07].

PKI consists of several components that support the establishment of a trust hierarchy and the binding of a user identity to a public key through the issuing of a Digital Certificate. Users, who do not inherently trust each other, need to be able to establish a level of trust in the public key presented to them as a token of another user's identity. This is the role of a recognised and trusted authority, aptly named a Certificate Authority (CA). The CA, in relation to electronic trust establishment, is what the identity and passport services of the world are to passport control at borders and ports. It is a third party, that issues identity tokens (passports) to individuals under its jurisdiction, and the identity authorities from other jurisdictions trust it as an identity verification authority, when they are presented with a set of identity credentials by an individual attempting to prove their identity at border controls. A CA will accept requests from individuals for a proof of identity, perform some level of identity verification, and then issue the individual with a Digital Certificate containing the individual's identity information and the public key to be used in cryptography. Before it is issued, the digital certificate is digitally signed by the CA with their private key. This allows anybody, who trusts that CA as a Source of Authority (SoA), i.e. they trust the CA to have performed the necessary identity verification checks and issued a valid identity document, to obtain the public key of the CA and verify that the certificate was in fact signed by the CA. This provides integrity in the binding of public key and identity to an individual. Users who do not trust each other establish their own trust relationship with the CA, and can then trust that any certificates issued by that CA are a valid identification of a user.

4.3.2. Existing Approaches to Access Control in VOs

The Virtual Organisation Membership Service (VOMS) [ACC+03] classifies authorisation information within VOs into two categories:

1. general information regarding the relationship of the user with their VO: groups they belong to, roles they are allowed to cover and capabilities they should present to resource providers
2. information regarding what the user is allowed to do, due to their membership of a particular VO

The authors suggest the first type of information should be contained in a server managed by the VO itself, while the second is probably best kept at the local sites, near the resources involved. This makes sense, as the VO is responsible for maintaining user groups and roles, while the owner of a shared resource will wish to keep the access control policy for their information private, and close to the physical location of the information. The VOMS service contains an administrative interface for modifying user roles and capabilities, thereby supporting dynamic control of access rights. This enables instant control over access rights through the creation and modification of user access privileges. This allows members of a VO to manage and maintain the VO credentials of its members and relate them to their role and status within the VO. It is separated from the management of access controls for resources shared within the VO, which can be mapped to the local access control policy of each member. VOMS and other existing technology, such as CAS and Shibboleth [PWF+02, Shib, WSJ07] provide a manageable solution to the first category of information. VO user relationships are well managed through such interfaces. The second category is the focus of this research, that is how information regarding user access privileges is managed, held and used to enforce access control both before and after information is shared in distributed collaborative environments.

4.3.2.1. Defining and Enforcing Access Control

Within VO environments, resource providers (VO members) specify their security requirements, i.e. a set of policies (rules) defining how information shared within the VO should be protected. This could be expressed through access control lists, rule or role-base controls in a number of different formats. These policies are stored at a Policy Storage Point

(PSP) and used when requests for access are made at a Policy Decision Point (PDP), to determine whether or not a requesting user should be allowed access to the resource [PCC+06]. User requests for access to controlled resources require details of user credentials (u_z), the identifier of the resource they wish to access (d_x), and an action(s) they wish to carry out to be sent to the PDP. This request is handled by a separate Policy Enforcement Point (PEP), which is used to accept access requests and invoke the PDP. The PDP invokes access control functions such as $f(u_z, d_x, a_i, r_o)$ or $f(c_{ku}, c_{kd}, a_i, r_o)$, depending on whether labels are used or not, and uses the function to evaluate access requests, using the rules defined and stored at a known PSP. PSPs effectively store rules such as those held in ACLs or Rule and Role-based access control lists. VOMS [ACC+03] is an example of this in practice. The outcome of this is an access control decision, as detailed in Section 4.1. In a VO environment, a project identifier and a VO identifier may also be included, so that the resource provider can make a decision based on the project and VO that the requesting user is coming from, rather than solely on the user's credentials.

Another current example of this approach in practice is the PERMIS [CO02] infrastructure for access control in distributed environments. The PERMIS infrastructure defines a Privilege Management Infrastructure (PMI), which can be likened to the Public Key Infrastructure (PKI), described earlier in this chapter. PKI is used to bind an identity to a certificate issued by a trusted authority. PMI extends the binding of identity to include user access privilege attributes for a particular identity. PMI defines Attribute Authorities (AAs), who issue digital certificates, similar to CAs in PKI. These certificates called Attribute Certificates (ACs), are stored in X.509 format, the standard format for digital certificates. The architecture software allows AA administrators to construct and sign ACs and store them in searchable, networked directories as PSPs, making them easily accessible when required by the PERMIS PDP to make access control decisions. Access control decisions in PERMIS are made using an authorisation policy, and for added integrity the policy itself is held within a signed AC. The AC contains a set of attributes bound to the owner of the certificate, defining the privileges granted to a subject by the issuing AA. The certificate is then signed by the AA to provide the set of privileges with integrity. The inclusion of all this information, and the signature of the issuer strongly bind the set of attributes to the holder, and anyone wishing to verify the integrity of this information can validate the digital signature of the AC, which is the Source of Authority (SoA). When a change in user circumstances occurs in a PKI controlled environment, the certificate of a user can be revoked. The same applies in this

case, as at any time, the AC for any user can be revoked, which means all the user's privileges are revoked. While the authorisation structure is the same as VOMS, the major difference between VOMS and PERMIS is the use of X.509 certificates to bind attributes and identity to a user. This effectively allows the VO to create their own PKI, where the user identity of the collaborators can be bound to a public key along with their role in the VO and even access privileges if that is deemed necessary. However, the use of public keys to hold access privileges may not be ideally suited to VOs, because it means any change in access privilege would involve revoking the public key and reissuing a new key with the new privileges. This removes some of the dynamism and flexibility of the VO environment and adds to the user management overhead.

The ISO 10181-3 Access Control Framework [ISO96], as followed by the PERMIS infrastructure, splits the functionality of an access control application into two components: the Access Control Enforcement Function (AEF) and the Access Control Decision Function (ADF). The PERMIS PEP performs the function of the AEF to deal with authentication, while the ADF is performed by the PDP as it makes an authorisation decision based on the access control policy for the organisation. It considers the identity of the subject making the request, the action requested to be performed on the target resource and other environmental factors such as time of day. The splitting of the two components is a natural division of tasks in an access control scenario. Authentication and Authorisation are two cooperating and intrinsically linked services, but research into the methods used to achieve the optimum functionality of each service is often separated into domain specific approaches. This division allows the selection and potential distribution of an appropriate mechanism to maximise the performance and flexibility of the access control application.

The ISO 10181-3 framework clearly splits access control decision-making and access control enforcement. Technology such as VOMS and PERMIS is evidently doing the same, defining a decision point (PDP) and an enforcement point (PEP) for access control. The access control enforcement (PEP) implementations are effectively enforcing decisions made by the PDP. PDP functionality maps directly onto the basic access control functions $f(u_z, d_x, a_i, r_o)$ and $f(c_{ku}, c_{kd}, a_i, r_o)$, which models access control decision-making. This is evident by the focus on users (u_z), resources (d_x), actions and rules. However, the PEP functionality must now also be included as it is crucial to supporting access control, which means extending the framework to include enforcement controls. Therefore:

Let D be a set of documents.

Let C be set of information classification schemes.

Let U be a set of users.

Let A be a set of actions (to be performed on a document).

Let R be a set of access control rules.

and

Let E be the set of all enforcement controls

The basic access control formula of $r_a = c_{ku} + \{=, >=, <=, >, <\} + c_{kd}$ for representing rules and function $f(c_{ku}, c_{kd}, a_i, r_o)$, still stand. e_b where $e_b \in E$ is any enforcement control that enforces access control decisions made using the access control decision function. Now that we have the addition of enforcement controls, we will investigate how enforcement controls are currently implemented and draw out any limitations in existing approaches, given the hypothesis that information can have its access control policy modified and enforced no matter where it is stored in an Internet connected environment.

4.3.2.2. The Centralised Perimeterized Approach

Both VOMS and PERMIS, together with other existing approaches to access control, such as CAS [PWF+02], Akenti [AKE] and VPMan [VPM] that deploy a similar approach, can be classified as Perimeterized approaches to enforcing access control. That is, they are perimeter-based protection mechanisms, and rely on the location of the target resource being kept under the control of an organisation within a secured information system perimeter. If the organisation wishes to share that information outside their secured perimeter, with these existing approaches, the PEP and PDP are no longer available as a mandatory barrier to enforce access controls. This is a major limitation in relation to controlling information in collaborative and distributed environments, where control of access to information is important, and there is a reliance on information sharing.

The introduction of perimeters as a factor in the implementation of enforcement controls requires the inclusion of virtual spatial concepts in the basic access control framework, namely domains and perimeters.

A perimeter in this context is the interface between Internet-connected users and organisation-owned documents. This is typically an organisation's network perimeter.

A domain in this context comprises a subset of all perimeters with a common and agreed information classification scheme and set of access control rules. For example, a domain could be a collection of organisations with common national purpose such as hospitals within the National Health Service or Government departments, or a wider international purpose such as the G8 forum.

An enforcement control in this context is a technology that makes *decisions* on whether to allow or deny document access to a user, and *enforces* the decision.

Thus, to extend the basic access control framework further:

Let I be the Internet-connected environment, as defined in Chapter 1.

Let M be the set of all domains within the Internet

Let P be the set of all perimeters

On the basis that I contains all machines that are connected to the Internet, let us call it the super-domain, within which all other domains are sub-domains. All organisations have perimeters. All domains have perimeters. However, a domain can be a subset of all perimeters, when comprised of several organisations.

A given organisation's perimeter was formulated in Section 1.2 as $P_a = \langle \{d_1 \dots d_n\}, \{r_1 \dots r_n\}, \{e_1 \dots e_n\} \rangle$, which defines a perimeter as a element within which a set of documents, rules and enforcement controls are contained. All documents have specific rules, which must be enforced by specific controls. Both the appropriate rules and controls must be present in order to enforce control on a document. The perimeterized approach to access control includes all approaches where control can only be enforced on documents while they remain *within* a perimeter that contains the appropriate rules and controls. Sharing rules is difficult when handling sensitive information, because the information owner is responsible for managing information access and usage, due to security requirements such as legal, reputational or intellectual property, to name a few. If rules move between perimeters, with existing approaches to access control, the owner loses full control of them. Thus, perimeterized approaches to access control are flawed for distributed collaborative working environments.

To identify a way round this limitation requires consideration of how access control is enforced in these perimeterized approaches. Access control enforcement can be either centralised or de-centralised. A centralised approach involves a single point of access control, where a centralised set of policies (rules) exists to enforce access control at a single location. In the case of a VO, this involves the VO members defining and agreeing to the access control policies for information shared within the VO. VOMS uses a centralised approach to access control. As discussed in Section 4.2, this approach has its drawbacks, such as the single point of failure if only one centralised access control point exists, meaning nobody can get access to any resources if it fails. It also means a large amount of user management is needed to manage all users of a VO from a single point, especially if the VO is dynamic and its users, roles and information protection requirements are frequently changing. Most importantly for collaborative VO environments, it also removes a lot of control from the owner of the resource. They will have some control over the rules that define access rights to their information, but ultimately if they are not the administrator of the VO, the control of information has passed to somebody else. This is not appropriate for sharing sensitive information.

4.3.2.3. The Decentralised Perimeterized Approach

A de-centralised approach involves moving parts of the access control infrastructure outside the centralised system. This allows more dynamism within the VO and less overheads in terms of user management, as well as removing the single point of failure issue. Welch et al. [WSF+03] present the concept of security as services, where authentication and authorisation processes are performed outside the perimeter and the results of the processes are returned to the perimeterized environment to control access. Sinnott et al. [SCD+08] present a comparison of the centralised model against the de-centralised approach, and detail the advantages of a de-centralised approach. In summary, in a de-centralised approach, access control policy for resources can be defined by the owners, rather than the VO members having to develop and agree on a VO-wide policy for all resources under centralised control. This occurs when a resource owner defines the access control policy and places responsibility with other remote (distributed) administrators within the VO, who they trust to issue users access rights based on this policy. This approach is called delegation and has been implemented in the DyVOSE project [WKSS06]. The use of delegation to issue and manage user access rights has the potential to reduce the user management overhead of resource owners within VOs, as each collaborating organisation within a VO will have an

administrator who will assign user roles and access rights to users under their control on behalf of the other administrators. In theory, this also means the remote users are assigned a more accurate set of access rights because the remote administrator knows and understands the rights required by their own users to carry out their duties and can more accurately issue rights. Delegation and de-centralisation of access control policy definition is particularly important in VOs for these reasons.

There are issues with a de-centralised approach. One is how VO members know where and how to locate and access resources without a centralised access point. Another is how roles defined by one VO administrator should be interpreted by other VO administrators. For example, if the role “manager” is defined by one administrator, how should other administrators interpret the access rights associated with that role? Centralised access control does not have these problems, so a hybrid of the two would create a solution that offers both sets of advantages, while removing most of the drawbacks. VOTES [SCD+08] creates a hybrid by using VOMS to manage user roles centrally, while using PERMIS to de-centralise access control policy decision and enforcement.

4.3.2.4. Limitations of the Perimeterized Approach

However, both centralised and de-centralised approaches are still based on perimeterization and can rely on the perimeter element formula $P_a = \langle \{d_1...d_n\}, \{r_1...r_n\}, \{e_1...e_n\} \rangle$ to contain documents, rules and enforcement controls. While the access control policy definition is returned, to some extent, to the owner of the resource in a de-centralised approach, the document is still required to remain within a secured perimeter to allow enforcement of the policy.

The limitation of the perimeterized approach, whether it be centralised or de-centralised, is the requirement for the document to remain within a perimeter to enforce policy. De-centralisation allows, what was previously a centrally defined and agreed access control policy to be decomposed, and control of its definition and enforcement to be returned to the owners of the information shared within a VO. To effectively control access to information outside the perimeter would require a de-centralised access control policy *and* system level enforcement controls to enforce policy, to not only be returned or moved to the resource owners’ systems, but to be present on the systems of anybody who has access to the distributed information. Effectively, the policy (rules) and controls need to travel with, or at least maintain control over, the information, wherever it goes. If this could be achieved, part

of the hypothesis, the claim that information can have its policy modified and enforced wherever it is stored in an Internet connected environment, could be supported.

This issue with this is that, in order for information owners to maintain control of their information, they must remain in control of the access control policy, which means the rules cannot be openly distributed, lest they lost control of them. Perimeterized enforcement controls act as a barrier between the user and the resource. Sharing documents outside the perimeter would require that barrier to remain available, so that access controls can be enforced. Thus, instead of being an identifiable, addressable endpoint, such as a centralised or de-centralised point of access control, the barrier itself has to be completely distributed, to the extent that it would have to be present or available to control access anywhere and on any machine to which information may be copied or moved. Thus, enforcement controls must be available on any machines to enforce policy, but the policy itself must remain centralised.

This can be achieved theoretically by redefining the perimeter and by making certain elements of the perimeter available within all other perimeters and domains in the Internet connected environment. The aim of this is to make documents, rules and enforcement controls available to everyone in all domains, and allow access control rules to be enforced outside the perimeter, while ensuring the information owner retains control of their information. Thus, the formula $P_a = \langle \{d_1...d_n\}, \{r_1...r_n\}, \{e_1...e_n\} \rangle$, which defines a perimeter as a subset of all documents, rules and enforcement controls, can be redefined as a new de-perimeterized element formula $P_z = D + \{r_1...r_n\} + E$, which means a single perimeter element contains the complete set of documents and enforcement controls, and a subset of all rules. This modification requires a change in thinking about segregation between computer networks. Previously, each perimeter had its own set of documents, rules and enforcement controls. Whereas, actually, it is the access control rules which are the only element that must remain perimeter-controlled. Documents can be shared and enforcement controls can be invoked as services or applications on demand [WSF+03], as long as *the correct rules for the document can be accessed and enforced*, while the rules remain under the control of the document owner.

The de-perimeterized element theoretically supports one of the claims of the hypothesis. Information could have its access control policy enforced wherever it is stored. It has been defined by identifying the weakness of perimeterized access and offers a new way of thinking about access control enforcement focusing on the decentralisation and distribution of

documents and policy control (rule) enforcement, where current thinking was focussed on decentralising policy development and decision making. The feasibility of achieving this will be discussed in Section 4.3.2.6, after the issue of granularity is discussed.

4.3.2.5. Granularity of Access Control

In addition to the perimeterization problem, there is also the issue of limitation on the level of granularity to which information resources within a VO can currently be protected. The most commonly implemented method of document security labelling is to take a label (c_{kl}) from a classification scheme, and assign it to a document d_x . This creates a document security label c_{kd} . This means the entire document is classified at a single level and user access can be restricted using the access control decision function $f(c_{ku}, c_{kd}, a_i, r_o)$, using rules defined using the basic access control formula $r_a = c_{ku} + \{=, >, <, >, <\} + c_{kd}$, as previously defined. However, this assumes that if a user meets the requirements of the formula, they should be able to access the entire document, and that all content within the document has the same security requirements. This is often not the case. For example, take an Electronic Patient Record (EPR) in a medical information-sharing scenario. The record comprises demographic patient details, medical history, current and previously taken medication, and long-term illness details. The information owner, for example a GP, may wish to share some of this information with a local hospital when referring a patient. Or, from a global view, a patient may become ill while abroad and the local hospital may require access to an EPR to understand a patient's reaction to a particular treatment. The GP, and in fact the patient, may not wish to share the entire record. Long term illness such as HIV or previous medication for depression is not relevant to anyone other than the GP and could be damaging to the patient's reputation if exposed. Therefore, only the parts of the document necessary for collaborative working should be shared. The basic access control formula becomes inappropriate at this point for information shared in distributed collaborative environments.

The entire-resource level of control can be compared to centralised access control policy development, where a single system defines the controls for the resource. De-centralisation means that multiple access control policies can exist, allowing information owners to specify different controls reflecting the varying levels of sensitivity of their shared resources. More sensitive content can be controlled with different controls to less sensitive content. This allows resource owners to classify their information according to its level of sensitivity.

Information resources themselves, particularly large resources, have the potential to contain content of varying levels of sensitivity. A resource owner may be forced to classify entire resources with a high level security label, when in fact a very small amount of the content within the resource requires high level classification. This affects the overall classification of the document due to the limitation of entire-resource controls, which ultimately limits the information that can be shared in collaborative VOs. If centralised access control policy development can be de-centralised, to allow resource owners to define different policies based on their own varying security requirements for the content within their resources, perhaps entire-resource controls can also be “de-centralised”, so that the owner of that information can define access control policy relating to different sections of the content, based on relative sensitivity, for example at a paragraph, line or even word level. This approach is very similar to that suggested in the Landwehr model (See Section 3.1).

To achieve this, we need to introduce the concept of sections of content within an overall document. Extending the basic access control framework further, we can add the concept of document sections:

Let d_{xy} be the y^{th} section of d_x ,

The basic access control formula $r_a = c_{ku} + \{=, >=, <=, >, <\} + c_{kd}$ only considers the label of the document (d_x) in its entirety, representing it as a single element of a classification scheme c_k . We need to change this by representing the document label a set of classification labels that are applied to different sections (d_{xy}). This can be done by extending the basic access control formula to include more than one label, creating a new **granular access control formula** $r_a = c_{ku} + \{=, >=, <=, >, <\} + c_{kd}$, where $c_{kd} \in c_k$. This formula can then either invoke the access control function $f(c_{ku}, c_{kd}, a_i, r_o)$ 1 to y times, where y is the total number sections in a document, and send each label to the function individually. Otherwise, the function could be modified to accept the set of all labels. Each section’s label from 1 to y is evaluated against the user’s security label c_{ku} , meaning the user may gain access to some parts of the document but not others. Extending the formula in this way to create the granular access control formula overcomes the granularity issue.

The granular access control formula theoretically supports another claim of the hypothesis, that a document’s content can have security enforced at different levels of granularity within the overall document. The rationale behind this formula is based on the theory of de-centralising access control policies such that information resource owners can control access

to their own resources and manage the access control policies within their own systems, and for their own individual resources. Community defined, centralised policies take away some of the owner's autonomy when defining access control for their resources as fellow collaborators have some control over the access control policies for the shared documents. Allowing the resource owner to have full control of the access control policy for their information allows them to classify and control their resources according to their sensitivity and restriction requirements. The granular access control formula takes this one step further and allows resource owners to classify and control content within a resource as well as the entire resource, giving them much more control over their shared content. It enables them to share content they were previously unable to share due to being classified at a higher level than was necessary, due to being in the same document as other highly classified content; and to share sections of content within a resource, such as an Electronic Patient Record, based on the information required by collaborators to perform their role in the collaborative working group, rather than giving them access to everything within the resource. This reduces the likelihood of potentially sensitive content being exposed. The granular access control formula, built on the basic access control framework, is another contribution of this thesis.

Research published by Damiani et al. [DCPS02] and Bertino et al. [BCF+04] focuses on breaking down the content of information resources, and applying controls to different sections of content with specific protection requirements. This allows the resource owner to classify the content of an information resource, and allow or restrict access, depending on who is requesting access. Rather than sharing an entire resource with a collaborator, these approaches allow only part of the resource to be shared, with the rest remaining restricted. This is particularly appropriate for enforcing access control in a distributed collaborative environment, as it provides the additional flexibility required by resource owners, to only share enough information so that a collaborator can perform the tasks required of them, without sharing information that is not relevant to them. This is required by the government [TW08] and healthcare information sharing [And08] scenarios.

The Damiani et al. approach is based on the perimeterized model, and thus does not provide the required de-perimeterized access control or implement de-perimeterized element formula. The Bertino et al. approach can support de-perimeterization and does follow the structure of the de-perimeterized element formula to some extent, by allowing documents and enforcement controls to be part of all perimeters while still enforcing access control. It works

by encrypting different sections of content with an individual key, meaning a role-based set of keys can be shared with collaborating users, based on their identity and information access requirement, allowing them to decrypt the information relevant to them, outside the perimeter. Both approaches rely on the resource being well structured, so that it can be broken down into different sections within the file data structure. As a result, both apply their approaches to XML-based information, a well-structured, standardized document format. It is this feature of both approaches that makes them particularly appropriate to this research, and the aim of finer-grained access control. XML is a standard specification language defined by the World Wide Web Consortium (W3C). Its syntax is structured, and can be used to form structured documents and messages. XML is platform independent and is accepted as the universal language for most Internet information exchanges. It is very flexible, allowing data to be structured into almost any representation. XML can be searched, parsed and tagged to pinpoint any data value held in an XML document. This document structure allows its content to be broken down, or fragmented, into subsections of information. The ability to break documents down into smaller, self contained sections of information is very useful when addressing the issue of granularity within current access control technologies, and is comparable to Landwehr's military message model.

XML documents consist of a number of hierarchical blocks of data. Each piece of information within the document is encapsulated within an XML *element*. A hierarchy of elements within the document makes each piece of information within the document individually addressable. When considering a Patient medical record, for example, Patient identity information, current medication, and medical history, can be held within separate XML elements. The Patient identity element can be broken down further into name, address and date of birth elements, which become a subset of the Patient identity element. Each element can be individually addressed using *XPath* path queries. For example, the path query *//Medical Record/Patient Identity/Name* would uniquely address the Patient name element of the medical record. This hierarchical, addressable data structure is an advantage of using XML to represent information. Damiani et al. and Bertino et al. use *XPath* queries and associate them with an access control policy. Thus, a document d_x can be fragmented into subsections $d_{xy}^{1...n}$, and the access control policy for information can be structured using a table of access control privileges, in the form of subject-object-action-sign, where *subject* is a user (u_z), *object* is the section of text identified by a path specified in an *XPath* query ($d_{xy}^{1...n}$), *action* is the action that is to be performed, and *sign* is a + or – indicating whether

the action is allowed or not. This once again follows the access control decision function and it can be extended to include the granularity controls. The aforementioned example path query could be used in an access control policy to define rules based on information at that location, thus individually controlling access to each element. Therefore both the Damiani et al. and Bertino et al. approaches follow an implementation of the granular access control formula and could support the implementation of that formula.

4.3.2.6. Managing Loss of Control

A drawback in the work of Damiani et al., Bertino et al., in relation to this research, is the lack of ability to retain sustained control over information in collaborative environments. Section 4.3.2.2 discusses the difficulty of sharing rules when handling sensitive information. If rules move between perimeters, the owner loses full control of them. The hypothesis states that access control policy for shared information must not only be enforceable outside the perimeter, but also modifiable. Perioellis et al [PCC+06] note that VOs by nature are dynamic and thus user authorisation needs to be inherently dynamic to properly support VO activity. Access rights should not be automatically assumed on assignment of a role within a VO. This supports the concept that the access control policy for shared information must be able to be modified, with the changes enforced on information already shared and stored on remote autonomous systems. Damiani et al. rely on a perimeterized model, where the information must remain within a secured network perimeter to be controlled. This does not support the concept of de-perimeterization within VO environments. Bertino et al. present an approach that could, in theory, be mapped to an implementation of the de-perimeterized element formula. They suggest the encryption of each section of an information resource based on the protection requirements for the section, with each section having its own encryption key. Based on an access control policy for the resource, information is then either requested (pull mode) through a centralised access control policy decision point, where the keys for decryption are presented to the user based on their credentials and relative access rights granted in the access control policy, or sent out to users (push mode) with the relevant keys for decryption accompanying the information. This is Role Based Access Control, based on the user's identity, credentials and access rights, granted within the access control policy. An issue with this approach is the number of keys that will be generated for each document, causing a potential key management problem. If a document is encrypted with several keys reflecting the different levels of protection required in the document, this could create a large

number of keys for an organisation to manage. Another issue is that the key distribution is permanent, that is, there is no way of revoking decryption keys once they have been distributed. This means that should an organisation wish to modify or remove access privileges to information at any time in the future, it would not be possible as, although the information is encrypted, the keys are permanently distributed. Thus, while access control can be limited to a certain set of users, the access control policy is not modifiable after key distribution.

The key to working around this problem, as defined in the de-perimeterized element formula $P_z = D + \{r_1...r_n\} + E$, is to distribute documents and enforcement controls, while keeping the rules within the protected perimeter. Referring back to the ISO 10181-3 Access Control Framework [ISO96], which splits the functionality of an access control application into two components: the Access Control Enforcement Function (AEF) or Policy Enforcement Point (PEP) and the Access Control Decision Function (ADF) or Policy Decision Point (PDP), they are separate but intrinsically linked entities. The enforcement point must be able to contact the decision point. Typically, in a perimeterized environment, the PDP (rules) and PEP (enforcement point) are known, addressable network entities. That is, they know how to contact each other within the perimeter. By moving the enforcement point outside the perimeter, the PEP and PDP lose contact, unless a link is maintained. This is something that must be overcome for the de-perimeterized element formula support secure information sharing.

Another approach to providing continuous control over distributed information, that is becoming increasingly prominent in commercial information systems, is Digital Rights Management (DRM) [Sta02, LSS03]. DRM techniques enable access and usage restriction controls to be applied outside the secure network perimeter, even if it is stored on media outside the control of the organisation that owns it. It works by defining an access control policy for a resource prior to its release, which remains effective throughout its lifetime and is distributed with the resource itself. DRM requires anybody outside the network perimeter to install proprietary software on their machine in order to access and use the information. This software acts as an extension of the organisation's information system as it is a distributed, policy decision and enforcement point. The policy (rules), PDP and PEP are kept together in one distributed package. It is the DRM software in this case that acts as the secure perimeter. DRM software, in this case, is an implementation of the perimeter formula $P_a = \langle \{d_1...d_n\}, \{r_1...r_n\}, \{e_1...e_n\} \rangle$. For example, when downloading music from somewhere like

iTunes, you cannot play the downloaded track without a limited licence, which is obtained on purchase and enforced using a proprietary media player loaded with the proprietary software. This restricts the sharing of the file on other machines. One drawback with DRM is the reliance on application and platform restraints. Users are subject to controls implemented by DRM vendors through specific software, and it cannot be assumed that all users in the working community will have access to the same application. For example, Microsoft have produced the Next-Generation Secure Computing Base (NGSCB) [MSFAQ] approach to DRM, but this cannot be used by somebody not working on a Microsoft based operating system, who wishes to provide DRM controls, when sharing information within a VO. For an implementation of the de-perimeterized element formula to be successful, where all enforcement controls are contained within all perimeters, the enforcement controls must be platform independent.

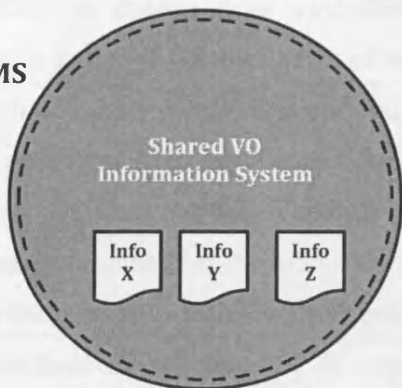
The DRM approach is also limited by the granularity of its controls. It is still restricted to controlling access to a resource in its entirety, meaning that an information resource can only be protected as a whole. It cannot support the implementation of the granular access control formula where document classification comprises a set of classification labels rather than a single label.

Another drawback with the current DRM technology is the lack of modifiable controls over the resource being protected. With an audio file, the controls for its use are unlikely to change so just enforcing the requirement for a limited usage licence through the use of specific software is suitable. In a VO environment, the requirements for control over shared files may change as the collaboration agreement in the VO changes. For example, if a document is shared with a VO member for collaboration purposes, the owner may want to protect its use. DRM can provide controls over system level operations, i.e. read, write, execute, copy, delete, and print, for the lifetime of the resource, giving the owner the option of restricting the use of their resource. However, at some point the owner may wish to revoke the ability of any collaborator to perform previously allowed system level operations. For example the owner may have lost trust in a collaborator and wish to revoke their ability to read this information. This action requires the ability to modify the access control policy and enforce it on previously shared information, which is not currently possible because with DRM the policy enforcement and decision points are both distributed in the form of a proprietary piece of software, together with the policy which is used by the software. In this case, the PEP and

PDP are still in contact, but the resource owner has been cut off from their information, therefore, not following the de-perimeterized element formula.

The concept of DRM goes some way to providing continuous control over distributed resources, through a trusted software client acting as the secure perimeter between the user and a resource. This supports the concept of the Clark-Wilson security model, which suggests the use of trusted software to enforce MAC controls. However, it still lacks the ability to modify the access control policy. The concept of a client tool that acts as a perimeter offers a solution as to how to completely de-centralise and distribute system level controls, but to facilitate a modifiable policy it is necessary for the resource owner to maintain control of the access control policy for the resource and enforce an up to date set of access controls.

Centralised e.g. VOMS



De-centralised e.g. PERMIS



De-Perimeterised e.g. DRM, Bertino

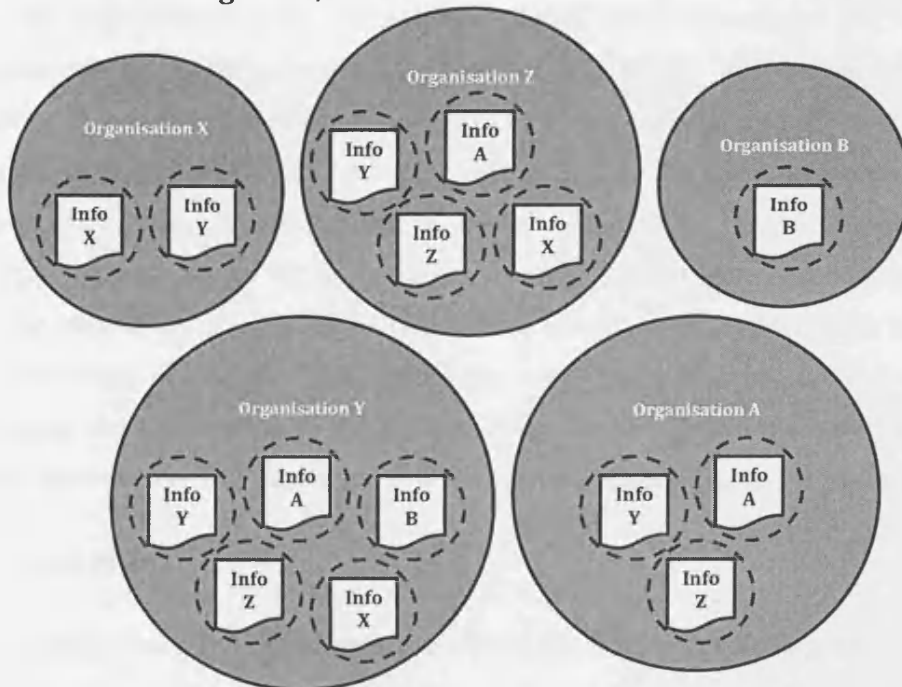


Figure 4.1 – Shift in Perimeter Control

Figure 4.1 shows the shift in control from centralised through de-centralised, to de-perimeterized approaches in terms of the perimeter of control over the information. In the centralised approach all shared information is controlled by a single PEP (the dashed line) inside a single network perimeter (the solid line). The policy that defines access control restrictions is defined by the VO, and the policy and all shared resources must remain within the perimeter to enforce access control. Information owners must give up complete control of their resources and store them outside their own perimeter, but within the perimeter of the VO system. In a de-centralised model, the PEP is returned to the organisations that are responsible for controlling access to the shared information. This occurs within their local network perimeters, where they maintain complete control of their information as the information and its access control policy is stored within their perimeter, while allowing shared access on the basis of retaining storage of the information. Both of these approaches are limited by the fact that the perimeters of control are fixed, and if the information is taken outside the perimeter, it can no longer be controlled. In a de-perimeterized model, the PEP and must be portable and the rules stored at a PSP and used by the PDP must be accessible by the PEP, so that the policy can be enforced outside the network perimeter and within other distributed network perimeters. The de-perimeterized element formula $P_z = D + \{r_1...r_n\} + E$, ensures the rules remain under the owner's control while documents and enforcement controls become part of all perimeters. However, to be able to modify access control policy, even after a document has been shared, and still be able to enforce changes to access control policy on information held by collaborating parties outside the resource owner's perimeter, there must exist a link between the PEP (e_b where $e_b \in E$), the PDP, which is bound to the access control policy $\{r_1...r_n\}$ for document d_x where $d_x \in D$, and the resource owner. Let us assume the resource owner is P_z as the perimeter is effectively a representation of a resource owner's boundary of control. This defines the relationship between all elements of de-perimeterized element formula. We can assume call this the **de-perimeterized linkage rule** that states there must exist a permanent link between a document d_x , e_b , $\{r_1...r_n\}$, and P_z .

4.4. Summary

Up to this point, the research presented has been focused on developing an access control framework and a set of formulae and rules to support the hypothesis. The hypothesis of the research:

A document's content can have security enforced at different levels of granularity within the overall document, and the rules defining its access control are always modifiable and enforceable in an Internet connected environment, no matter where the document is held.

There are three claims in total:

- i) security can be enforced at different levels of granularity within a document,
- ii) access control policy can be enforced outside the perimeter, no matter where it is stored within an Internet connected environment, and,
- iii) access control policy can be modified and ii) is still applicable

The basic access control framework is as follows:

Let D be a set of documents, of which d_x is a document element that can be assigned a single label c_{kd} or a set of labels c_{kd} , where $c_{kd} \in C_k$, when classified at a granular level on its sections d_{xy}

Let C be a set of information classification schemes, of which c_k is a classification scheme used within a perimeter or domain.

Let U be a set of users, of which u_z is an element that can be assigned label c_{ku}

Let A be a set of actions (to be performed on a document), of which a_i is a specific action element

Let R be a set of access control rules, from which a subset of rules $\{r_1...r_n\}$ can be defined to support an organisation's access control policy

Let E be the set of all enforcement controls, of which e_b is an enforcement control element

Let I be the Internet-connected environment, as defined in Chapter 1.

Let M be the set of all domains within the Internet

Let P be the set of all perimeters

These are the components required to frame the level of thinking necessary to support the claims of the hypothesis. Using these components, two formulae and an associated rule have been derived to theoretically support the claims.

The granular access control formula $r_a = c_{ku} + \{=, >=, <=, >, <\} + c_{kd}$, where $c_{kd} \in c_k$, represents a user (u_z) being assigned a classification label (c_{ku}) from a classification scheme (c_k), which has some relationship to the classification labels used to classify the sections of content (c_{kd}) within a document (d_x). Each section (d_{xy}), within a document can be classified with its own label by using a subset of labels to represent the security requirements of the document, rather than a single label. The access control function $f(c_{ku}, c_{kd}, a_i, r_o)$ will evaluate each label against the user's label to determine whether access should be granted or not, in support the enforcement of security at different levels of granularity within a document (Claim (i)).

The de-perimeterized element formula $P_z = D + \{r_1...r_n\} + E$ represents all enforcement controls (E) being available within all perimeters (of which P_z is a single element), to support access control policy enforcement on all documents (D) stored outside the perimeter, no matter where it is stored within an Internet connected environment (Claim (ii)).

The de-perimeterized linkage rule which states that there must exist a permanent link between a document (d_x), the appropriate enforcement controls (e_b), its access control policy $\{r_1...r_n\}$ and its the owner (via their perimeter) (P_z) supports Claim (iii).

To test the feasibility of implementing these formulae and rules, the next Chapter documents an implementation of a prototype application that aims to implement them.

Chapter 5 - An Enhanced Approach to Access Control for VOs

To enhance current information security capability in support of more secure information sharing in collaborative distributed environments, the hypothesis of this research makes three claims, and the research so far has produced two formulae and a rule, based on an access control framework, in support of these claims. :

- i) security can be enforced at different levels of granularity within a document,

$$r_a = c_{ku} + \{=, >=, <=, >, <\} + c_{kd}, \text{ where } c_{kd} \in c_k$$

- ii) access control policy can be enforced outside the perimeter, no matter where it is stored within an Internet connected environment, and,

$$P_z = D + \{r_1 \dots r_n\} + E$$

- iii) access control policy can be modified and ii) is still applicable

There must exist a permanent link between a document d_x , e_b , $\{r_1 \dots r_n\}$, and P_z

This chapter details the development and implementation of a prototype system that aims to implement these formulae and rules to demonstrate the feasibility of their implementation. The rationale behind doing this is that, if they can be implemented, it would provide a strong argument in support of the hypothesis.

Additionally, Chapter 3, the study of existing access control models, identified some desirable features that would exist in a security system for distributed collaborative information sharing. These are shown for reference in Figure 5.1. There were a number of features that came from the multi-level and multi-lateral models. The label-based approach of multi-level is supportive of advanced access control granularity, to the content level inside a document. While the Clark-Wilson model of application-level controls and audit logs is supportive of client-PEP controls such as those developed in Digital Rights Management. The key thing that is missing in existing technology is the ability to conform to the de-

perimeterized linkage rule, which requires a permanent link between d_x , e_b , $\{r_1...r_n\}$, and P_z . This is something that the prototype system will aim to overcome. We will begin with an approach to achieve this.

- Classify users and assign labels based on the levels of access they are allowed, in order to define the maximum level of information a user can access. This is based on the strengths of the Bell-La Padula and Biba models. It limits user access to information, when access is not required to carry out their tasks in an organisation.
- Classify content within information resources to a much finer-grained level, in line with the Landwehr model for access control. This allows content with varying levels of sensitivity to be classified at different levels in the same resource, and also allows contributors to an information resource to classify their own information, with their own protection requirements.
- Support classification label interoperability between organisations, so that classifications defined by one organisation can be interpreted by another organisation when accessing and handling information. This is an issue from studying the application of Denning's lattice, in collaborative environments, between multiple organisations.
- Be implementable as machine enforceable controls, so that classification labels can be related to access control restrictions, and controls can be enforced. This would enable mandatory access control through a software infrastructure, as suggested by Clark and Wilson's separation of duties model.
- Support an audit trail by logging user access requests, as suggested by Clark and Wilson's well-formed transaction model. In the case of information misuse, an audit can be performed to analyse actions which determine the acting parties.
- Ensure that information is not released to collaborating organisations that have a conflict of interest, based on the Chinese Wall model.

Figure 5.1 – Desirable Features of an Access Control Model

5.1. Achieving the Link that Obeys the De-perimeterized Linkage Rule

Linking information to a usage control policy is something that has been achieved by the Creative Commons community [AALY06]. Rather than an access control policy, Creative

Commons defines an acceptable usage policy and associated license for distributed information. It comprises a set of icons, embedded in a shared resource, that inform the reader of their obligations and limitations when sharing and reusing the information. For example, there are icons that represent “no profit must be gained from its use”, and “no derivative work may be based on it”. The approach embeds a URL within the resource that links to a document detailing how the reader should interpret the icons, and adhere to the usage policy. This is a live URL and, of course, can be updated and modified at any time, should the meaning of the icons change. There are no technical controls that enforce the Creative Commons licenses; rather the licenses are represented in human, machine and lawyer readable form, such that any information misuse can lead to prosecution.

To achieve retention of access control for shared information, it could be possible to build on the Creative Commons approach of linking what are effectively classification labels to an acceptable use policy for shared information, and modify it to replace the acceptable use policy with an access control policy. This could provide the necessary link between PEP, PDP and resource owner and satisfy the de-perimeterized linkage rule. The PEP could be distributed as a client-side piece of software that enforce policy decisions, while the access control policy and PDP could remain under the control of the owner, rather than distributing the policy, PDP and PEP, as DRM does. The link between PEP and PDP could be provided by embedding a URL in the document before it is shared, as Creative Commons does. This link could be accessed by the PEP and used to connect it to the centralized PDP and policy. By doing this, the policy remains under the control of the information owner and is modifiable, while the PEP can get the latest version of the policy each time an access control request is made. With the PEP being an enforcement control (e_b) in relation to the access control framework, the de-perimeterized access control formula can be satisfied, so long as the control is accessible outside the perimeter. Section 4.3.2.3 details the concept as suggested by Welch et al. [WSF+03] of security as services, where authentication and authorization processes are performed outside the perimeter, and the results of the processes are returned to the perimeterized environment to control access. There is no reason, why policy enforcement couldn't also exist as a service, using Web Services techniques (see Chapter 2) to codify similar controls to those deployed in perimeterized environments, as a client-side application. This is effectively how DRM works. However, DRM lacks the ability modify policy. This could be overcome using the approach discussed in this section.

The system developed in support of demonstrating the feasibility of the new formulae and rules breaks access control policy down into two distinct but related elements. These are: a distributed element, and a centralised access control matrix. The distributed element utilises classification labels, following the access control models of Bell-La Padula and Biba. The labels are embedded within the body of a distributed information resource, building on the work of Creative Commons. The labels relate to a centrally managed access control matrix. The matrix defines the identity attributes required to gain access to content within the resource that has been classified with security labels. This matrix remains at a centralised location, where the mapping between classification labels and identity attributes can be modified at any time to add or remove access privileges to classified information, while the classification labels remain permanently within the body of distributed information. The important part in making the access control policy enforceable outside the perimeter is to maintain the link between the matrix and the classification labels after distribution. This is made possible through the technical mechanisms described in this chapter.

5.2. De-Perimeterized Security - Architectural Components

The functional architectural components within the basic access control framework are as follows:

Let C be a set of information classification schemes, of which c_k is a classification scheme used within a perimeter or domain.

Let R be a set of access control rules, from which a subset of rules $\{r_1..r_n\}$ can be defined to support an organisation's access control policy

Let E be the set of all enforcement controls, of which e_b is an enforcement control element

The following sections explain the development and implementation of a set of technical mechanisms encompassing these components and identify the key advancements to existing methods and approaches, which distinguish these developments from other work and contribute to the information security domain.

5.2.1. Information Classification Scheme

People within organisations have various roles. With these roles come varying levels of responsibility and a requirement for access to information necessary to carry out the duties of the role. The various roles in an organisation will have different levels of access to restricted information. It is more important to restrict access to some information content than others, from the data controller's point of view. This depends on its value to the organisation, and the legislation and regulation that controls its use. A lattice or matrix structure is formed involving people (subjects) and information (targets), which maps from the roles available to any given subject and the information that is of a restricted nature. Research documented in Chapter 4 has shown the evolution of access control from simple access control lists to complex rules, and currently to access control rules based on a set of roles. Roles are usually decided by replicating the organisational employee hierarchy of the real world, where people are given roles that allow them to assume privileges within the organisation to carry out their jobs. However, in domains such as healthcare and Government, information is much more complex than a single entity containing content to which a single classification label can be applied and a single role allowed access. Consequently there should be functionality available to split content into sections, which are classified according to their confidentiality and integrity protection requirements. As a result of this functionality, subjects should be able to access limited amounts of information within a resource based on their identity and role within the organisation. To be able to make this sustainable, scalable and usable throughout an organisation, and to support its enforcement through interpretation by a human and software infrastructure, the classification needs to be carried out under the guidance of a specific and concise set of rules that encapsulate the necessary security requirements that apply to the roles defined within the organisation. This set of rules is known as an Information Classification Scheme or ICS.

Perhaps the most widely known ICS is the military/governmental scheme shown in Table 5.1, which is taken from [Brag06]

Classification	Description
Top Secret	Disclosure of top secret data would cause severe damage to national

	security
Secret	Disclosure of secret data would cause serious damage to national security. This data is considered less sensitive than data classified as top secret
Confidential	Confidential data is usually data that is exempt from disclosure under laws such as the Freedom of Information Act, but is not classified as national security data
Sensitive But Unclassified (SBU)	SBU data is data that is not considered vital to national security, but its disclosure would do some harm. Many agencies classify data they collect from citizens as SBU.
Unclassified	Unclassified is data that has no classification or is not classified as sensitive

Table 5.1 – Governmental Classification Scheme

Considering the potential benefit of the Bell-LaPadula and Biba models for access control, the military classification scheme seems a good starting point for designing an ICS. Its classifications are clear and distinct, however, as Clark and Wilson observed [CW87], they are not all relevant to the commercial world, and there is no flexibility within them to allow commercial concepts or restrictions to be applied. For example, there is no classification for proprietary information that is confidential, but which can be released under certain licensing conditions that restrict its use. Clark and Wilson also noted that commercial information cannot necessarily be classified solely in terms of confidentiality (exposure). The integrity of information is sometimes just as important in the commercial sector when considering the impact of uncontrolled editing of information. Not only must the information be protected against unauthorised eyes seeing it, it must also be protected from being written to by unauthorised people, where its correctness and completeness could be damaged. The

classification scheme used in a VO information sharing scenario, would ideally reflect the dynamic and flexible nature of the VO itself, and so must contain a set of classification labels that reflect differing levels of confidentiality and integrity.

There is no globally agreed standard for classification of commercial or nongovernmental information. In this case, the level of classification is dependent on the discretionary level of restriction required by the owner of the information, and the desired level of confidentiality and integrity. [Brag06] defines a set of commercial data classifications, that provide a range that could be used to provide further levels of granularity from highest to lowest as shown in Table 5.2.

Classification	Description
Sensitive	Data that is to have the most limited access and requires a high degree of integrity. This is typically data that will do most damage to the organisation should it be disclosed
Confidential	Data that might be less restrictive within the company but might cause damage if disclosed
Private	Private data is usually compartmental data that might not do the company damage but must be kept private for other reasons. Human resources data is one example of data that can be classified as private
Proprietary	Proprietary data is data that is disclosed outside the company on a limited basis or contains information that could reduce the company's competitive advantage, such as the technical specifications of a new

	product
Public	Public data is the least sensitive data used by the company and would cause the least harm if disclosed. This could be anything from data used for marketing to the number of employees in the company

Table 5.2 – Commercial Information Classification Scheme

This set of classification labels offers more to the commercial classification of information than the military/governmental model because it includes commercial factors, such as proprietary information. However, the classification is still very much focussed on creating a superficial label that is applied to a target, which is aimed at identifying its protection requirements. As Clark and Wilson identified [CW87], commercial information depends on its integrity, while the military approach is heavily based on confidentiality. These requirements continually emerge as the two most important aspects of information assurance from an access control perspective. Confidentiality is the requirement that only authorised users can view information. Integrity is the requirement that only authorised users can modify information. Thus, the classification scheme should ideally encompass both requirements. In a collaborative working environment where both confidentiality and integrity are important, it may be prudent to select a label for each and assign them to a user. For example, using the military classification scheme as an example, a user might be able to read ‘Top Secret’ information, but not write to it. Their write label might be capped at ‘Secret’. However, this goes against the rules of Bell-LaPadula and Biba, which restricts read and write access to information classified with a single label. Both of these classification schemes are hierarchical, meaning the classifications get more restrictive higher up the list of labels. Organisational roles are also typically hierarchical. For example, office junior, manager, senior manager, and chief executive are hierarchical roles and, as such, the hierarchical classification schemes are appropriate. They follow a multi-level security model, enforced using the rules of Bell-LaPadula and Biba. The objective of sharing information in collaborative distributed environments is to enable collaborators to be able to perform the duties required of them to achieve the goal of the collaborative working group. This is task oriented, not hierarchical. It may be feasible that an office junior from one organisation and a

chief executive from another, are using the same information to complete a collaborative effort. Therefore, it is the information circulation requirements across multiple domains that are important in deriving its security requirements. Multi-lateral security models may be more appropriate in this case, restricting information flow between domains, rather than between hierarchical levels.

A classification scheme that is particularly appropriate for classifying information to be shared across multiple domains, and which could support a multi-lateral flow of information control using separate controls for confidentiality and integrity, is the Traffic Light Classification Scheme, as used by the G8 Nations [JF09]. This protocol has now been accepted as a model for trusted information exchange by over 30 countries. The protocol provides four information sharing levels for the handling of sensitive information. The four information sharing levels are:

- RED – Personal. For named recipients only.
- AMBER - Limited distribution. This can be interpreted as a requirement to share within a collaborative working arrangement or VO.
- GREEN - Community wide. The circulation of this information is still limited, but in a broader sense than amber. This could be interpreted as within or between specific organisations.
- WHITE - Unlimited. May be distributed freely, without restriction.

These levels do not focus on assigning a hierarchical level to information. Rather they focus on circulation requirements, that is, which groups of people can access information. The meaning of the labels remains the same between all organisations, so the sharing requirements are clear. This alleviates any confusion of label meaning that might arise between organisations. For example, if an organisation receives a resource classified as ‘Secret’, it is unclear whom they can share it with. Does this mean ‘Secret’ within the organisation, or ‘Secret’ across organisations? Can they discuss this with colleagues? Using the traffic light scheme, they know that ‘Amber’ classified information should only be shared within a collaborative working group, and not with other colleagues who are not involved in the collaboration. Likewise, ‘Red’ allows information to be shared with specific individuals. Even the highest level of military classification cannot support this. In collaborative working groups, this is particularly appropriate because, as the consortium develops, there may be information that begins as restricted to a number of named recipients, which later expands to

all members of a particular working group, and finally, expands to specific organisations. The red, amber and green levels support this. Also, confidentiality and integrity can be handled individually. For example, 'Amber' information may be shared with the entire working group, but only edited by specific 'Red' individuals.

Information can be classified based on its value to an organisation in terms of financial, legal, operational or reputational impact if data misuse occurs. The factors affecting the choice of label could be relative amounts of system downtime, lost sales, threat to users and so on, with the major unit of measure potentially being cost or loss of life.

Using the basic access control framework, (c_k) can represent the schema shown in tables 5.1 and 5.2, the military and commercial classification schema, as well as the Traffic Light Scheme. It is classification scheme agnostic. Any of the schemes could be used to make access control decision using the basic access control formula and, importantly, the granular access control formula. Read and Write controls can have separate rule-bases and access can be based on role, identity or any other user credential, by representing it as u_x . The important point to note is that classification schemes must be agreed between collaborators before information is shared. The access control decision formula only holds true if an agreed classification scheme is achieved. Agreeing terms and conditions of a classification scheme is beyond the scope of this work but may be considered in future, as the basic access control framework provides a good basis for research into mappings between different organisational classification schemes and enforcement controls.

For the purposes of demonstrating the feasibility of implementing the granular access control formula, the traffic light classification scheme is used in the prototype system. The traffic light schema is ideally suited to be a worked example because of its context-free nature, that is, the colours could have various meanings either in a multi-level or multilateral sense. However, the hierarchical model used in the military or commercial ICS is equally applicable. This thesis is not arguing the case for any particular ICS to be adopted. It aims to be agnostic of ICS.

The purpose of the prototype is to demonstrate the feasibility of implementing the formulae and rule developed in support of the hypothesis. The granular access control formula (claim (i)), supports the concept of finer-grained access control and enables a person wishing to classify information to evaluate the importance of the information within a resource and select classification labels for the sections of information they feel should be restricted to

anyone, who does not possess the required identity attributes. The application requires subjects requesting access to supply specific identity information. To enable a range of controls on identity, Digital Certificate identity attributes have been used as authentication credentials, to enable the establishment of trust in an identity, and create a range of identity based controls when defining access control policy. The identity attributes able to be extracted from digital certificates are an:

- individual name,
- organisation, or
- VO identifier.

Thus, permutations of access control rules in collaborative environments can be supported, where control can apply to an individual, based on their role; an entire organisation, based on its role, or a VO working group in its entirety. This supports scenarios where information can be shared VO-wide, or restricted to a selection of collaborating organisations within a VO, or even further, to the individual person level within an organisation or a VO. This offers much more flexibility than a simple username and password. All of these can relate to u_z in the access control framework.

Subjects (u_z) may obtain privileges to view (confidentiality) or modify (integrity) content within a document (d_{xy}), classified with a particular label. Thus, supporting advanced access control to achieve fine grained access control to paragraph, line or even word level, based on identity attributes.

Consider the set of identity attributes in Figure 5.2 that are used for access control decision making. The identity attributes held by subjects wishing to access information resources, map onto a matrix of classification labels that define the identity or role based attributes required to gain access privileges to information classified with those labels. For example, anyone with the identity attribute (u_z) “Cardiff University” as an “Organisation Name” may be granted read access to information classified as RED ($D_{xy} = \text{RED}$), but only those with a “VO Identifier” attribute of “Teaching Working Group”, which defines a particular role within the organisation, may be granted write access to information classified as RED.

Subject Identity Attributes
Personal Name
Organisation Name
VO Identifier

ACCESS CONTROL MATRIX		
Identity Attributes	Read	Write
Joe Bloggs:Cardiff University:Teaching Workshop Group	RED:AMBER:GREEN	RED:AMBER:GREEN
Dave Binks:Cardiff University:Development Workshop Group	RED:AMBER:GREEN	AMBER:GREEN

Figure 5.2 – Policy Attributes and Values

Note that each classification label is stored individually in the access control matrix. A traditional hierarchical classification scheme would automatically allow access to AMBER and GREEN labels if the subject had RED access. In this case the controls available are much greater because each label is controlled in its own right. In theory, a subject could have read access to RED and GREEN, but not to AMBER. This means that, in future, the labels could relate to other controls in addition to the basic read control. For example, GREEN access could mean full access allowed, AMBER – time based access, only between the hours of 9 and 5, and RED - the country the access request is coming from must be the UK.

The identity information is provided to a user and bound into a Digital Certificate from a locally hosted VO through a PKI service, described in the PERMIS architecture in Section 4.4.2.1. This allows identity details to be trusted by all VO members, who trust the issuing PKI service for the VO.

A matrix exists for each document. The rules represented in Figure 5.2, using the granular access control formula $r_a = c_{ku} + \{=, >=, <=, >, <\} + c_{kd}$, where $c_{kd} \in c_k$ for context are:

For all sections ($y^{1...n}$) within d_x , user Joe Bloggs ($u_{JoeBloggs}$) has a Read label c_{ku} and Write label c_{ku} of Red, Amber and Green.

For all sections ($y^{1...n}$) within d_x , user Dave Binks ($u_{DaveBinks}$) has a Read label c_{ku} of Red, Amber and Green, and Write label c_{ku} of Amber and Green.

So if section y , within document d_x , has a classification of Red i.e. $c_{kd} = RED$, using the function $f(c_{ku}, c_{kd}, a_i, r_o)$, given the user Joe Bloggs and the action write, the function call would be

$f(\{Red, Amber, Green\}, \{Red\}, \{Write\}, \{Reference\ to\ ruleset\ as\ shown\ in\ Fig.\ 5.2\})$, and would result in access being allowed.

5.2.1.1. Implementing the Granular Access Control Formula

As published by Damiani et al. [DCPS02] and Bertino et al. [BCF+04], the method for applying classification labels to the body of proprietary information lies in the flexibility of XML. Because of its structured nature, XML can be used to encapsulate information into nested sections. XML data is structured in such a way that it has related elements that open and close around sections of content, with all information between the elements being encapsulated within. This allows sections of content to be fragmented into separate chunks according to the protection requirements of the content. Each opening XML element can contain attributes, which make the addition of tags possible within the body of an XML document. A major issue is that most information resources are saved in a proprietary format. Microsoft is the predominant product within most organisations for electronic information processing and the file format is interpretable only to other Microsoft products. However, with the increasing adoption of service oriented architectures that use XML as their information exchange language, even Microsoft are moving to a similar format creating an open standard called Office Open XML or OOXML [ECMA08] as the file format for their Office 2007 suite. This format is an interpretation of XML which can be transformed into raw XML through various schemas. For legacy Microsoft document formats, and many other proprietary formats, there are multiple releases of free software such as DocVert [DV] that can convert proprietary documents into raw XML that can be manipulated for this purpose.

As a working example, consider the sample document shown in Figure 5.3. It is made up of paragraphs of text in normal presentation format - a title and three paragraphs of text with different confidentiality and integrity assurance requirements that are self explanatory when reading the text. The sample excerpt is taken from a Microsoft Word document and would be saved in the format associated with that. This means nothing can be added to the document by a user that could be hidden away or transparently manipulated by the system, as would be required to support the addition of security labels.

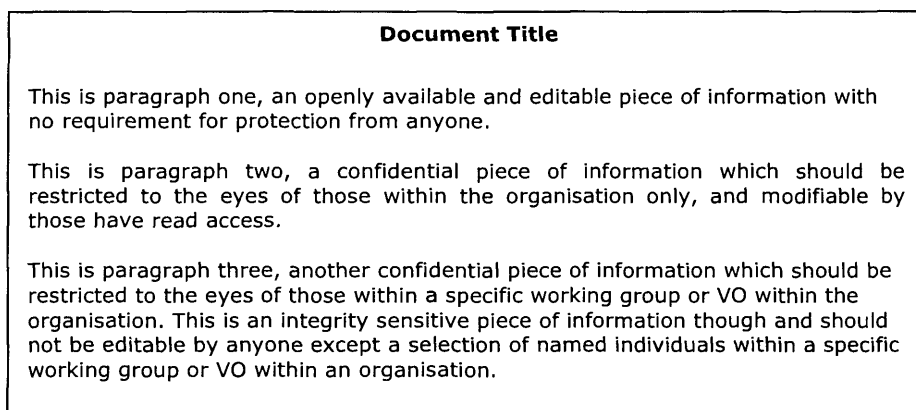


Figure 5.3 – Paragraphs of text in normal format

The prototype system handles proprietary data by converting the entire document into an XML format that would allow such manipulation. This is made possible by using software services, such as DocVert, which provide a Web Service to accept proprietary files as input, and convert the proprietary document into raw XML format. Figure 5.4 shows the same document after this conversion has taken place. Each paragraph is now held between its own XML elements that open and close around the paragraph.

```
<?xml version="1.0"?>
<db:book xmlns:db="http://docbook.org/ns/docbook">
<db:preface>
  <db:para>Document Title</db:para>
  <db:para>
    This is paragraph one, an openly available and editable piece of information with no
    requirement for protection from anyone.
  </db:para>
  <db:para>
    This is paragraph two, a confidential piece of information which should be restricted to
    the eyes of those within the organisation only, and modifiable by those have read
    access.
  </db:para>
  <db:para>
    This is paragraph three, another confidential piece of information which should be
    restricted to the eyes of those within a specific working group or VO within the
    organisation. This is an integrity sensitive piece of information though and should not
    be editable by anyone except a selection of named individuals within a specific working
    group or VO within an organisation.
  </db:para>
</db:preface>
</db:book>
```

Figure 5.4 – The same paragraphs in XML format

While Damiani et al. [DCPS02] and Bertino et al. [BCF+04] used XPath queries to define policies that reference precise sections of content within XML, it is also important to note that XML elements, such as the <db:para> element, can have multiple attributes associated with them, which can store extra information about that element. This feature of XML allows the information classification labels to be bound to the information. Figure 5.5 shows how the XML can be modified to include the classification labels for the information based on the traffic light information classification scheme.

To add labels to information, a Graphical User Interface (GUI) to interface with the application has been developed, so that an information owner can use the GUI to open a document, highlight sections of text and then select an information classification label from a list. On saving the document, the underlying *information labelling mechanism* dynamically embeds the chosen label into the information at the relevant point, to encapsulate the selected information in a classified container, as shown in Figure 5.5.

```
<?xml version="1.0"?>
<db:book xmlns:db="http://docbook.org/ns/docbook">
<db:preface>
  <db:para>Document Title</db:para>
  <db:para>
    This is paragraph one, an openly available and editable piece of information with no
    requirement for protection from anyone.
  </db:para>
  <db:para label="AMBER">
    This is paragraph two, a confidential piece of information which should be restricted to the eyes
    of those within the organisation only, and modifiable by those have read access.
  </db:para>
  <db:para label="RED">
    This is paragraph three, another confidential piece of information which should be restricted to
    the eyes of those within a specific working group or VO within the organisation. This is an
    integrity sensitive piece of information though and should not be editable by anyone except a
    selection of named individuals within a specific working group or VO within an organisation.
  </db:para>
</db:preface>
</db:book>
```

Figure 5.5 – The same paragraphs, in XML format with addition of sensitivity labels

The information now has embedded classification labels encapsulating content within the overall resource that is particularly sensitive, and is required to be protected differently from other content within the same resource. The choice of label is driven by the ICS for an organisation and is representative of the impact of the information not being appropriately protected. This example also illustrates how information sharing is limited without the advancement of access control to the information content level. File-level classification would force the entire resource to be classified as RED because of the small amount of content classified RED within the resource. Information-level labelling allows the RED content to be classified differently to the rest of the content, and further levels of sensitivity to be supported.

5.2.2. Access Control Policy Generation

Once the labels have been embedded, the document enters its *controlled* state. From this point on, the access control model considers the requirements of the system threat model (Section 2.4.2) in order to maintain information security in a de-perimeterized environment. The first action is to secure the information, both the resource content and classification labels, against unauthorised access outside the perimeter. This is achieved by encrypting the entire resource, content and labels. The encryption algorithm used is AES, with a 256-bit key. This configuration was chosen because it is currently unbreakable at the time of writing. The symmetric encryption/decryption key is stored locally in a table that maps the encryption key to a resource identifier. Each resource has a unique resource identifier generated when it first enters its controlled state. The resource identifier is appended to the encrypted resource in clear text, so that it can be extracted by the *policy enforcement mechanism* and mapped onto the table of keys to obtain the decryption key.

Next, given the nature of an information sharing environment, where the information should now be able to be shared with collaborators outside of the perimeter of its owner, and in order to support the de-perimeterized access control formula and de-perimeterized linkage rule, it is essential to embed a link into the information that maintains a link between the distributed resource, more specifically the security labels in the resource, and the centralised access control matrix. This link allows the owner to maintain continuous control over access to their classified information through the *policy enforcement mechanism*. The existing perimeterized approach works by accepting access requests from subjects wishing to gain access to information stored within the perimeter. The perimeter has an interface through which access

requests are accepted, and access control decisions are made within the perimeter. If access is allowed, the subject gains access to the information held within the perimeter. If the information moves outside the perimeter, the barrier between subject and information is removed and the subject can gain full access to the information. The prototype application shifts the perimeter to the distributed *policy enforcement mechanism*, which is effectively a distributed PEP. Instead of a subject going directly to the perimeter interface to request access, they interface directly with the policy enforcement mechanism, which interfaces with the centralised access control matrix through a Web Service interface hosted by the information owner. The location of this interface, known as the Policy Decision Point (PDP), is embedded into the resource in cleartext, along with the resource identifier, so that it can be extracted by the policy enforcement mechanism when access requests are made.

Finally, an access control matrix is created for the classified resource. The matrix is linked to the resource through the resource identifier and contains a list of known subjects for which access control will be enforced. The GUI developed to demonstrate the prototype system provides a policy management interface that allows the information owner to select subject identities and define the classification labels to which they should be allowed access for any given resource. As the information owner makes these decisions through the GUI, the *policy definition mechanism* instantly and transparently updates the access control matrix for the resource to reflect access and modify privileges for subjects, as they are added or removed.

5.2.3. Access Control Policy Enforcement

A distributed policy enforcement point was developed to support the implementation of the de-perimeterized access control formula. A GUI was also created to provide a user interface to the PEP. Subjects who wish to gain access to distributed information must use the PEP GUI tool to request access, as the information is rendered unusable until they do so. This can be executed on a remote client by downloading and running the GUI. It will run on any operating system because it is written in Java. It runs from a self-executing file, meaning no installation is required. This is an advantage because information system administrators often limit the installation of proprietary software on machines under their control.

5.2.3.1. Implementing the De-perimeterized Access Control Formula and De-Perimeterized Linkage Rule

As shown in Figure 5.6, the *policy enforcement mechanism*, initiated by the GUI upon requests for access, extracts the cleartext from the resource, which includes the location of the PDP for the resource, and the unique resource identifier.

The mechanism then extracts the requesting user's identity credentials from their Digital Certificate. The subject must configure the location of their certificate before any access requests take place.

Next, the mechanism creates an access request, containing the resource identifier and the requesting user's identity credentials, and sends it to the PDP at the location extracted from the resource. Figure 5.7 illustrates how the PDP service maps the request onto the relevant access control matrix, using the resource identifier from the request to locate the correct matrix.

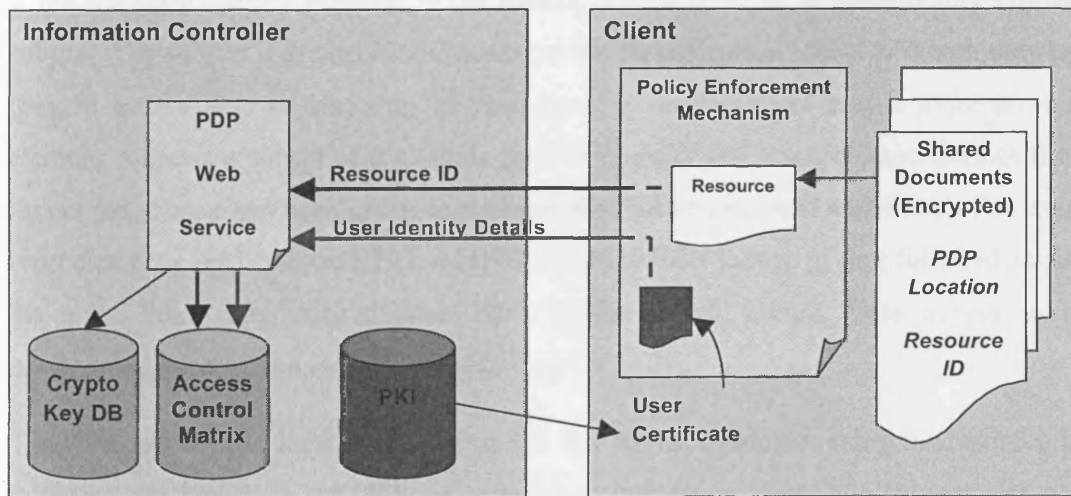


Figure 5.6 – Conceptual Architecture Overview

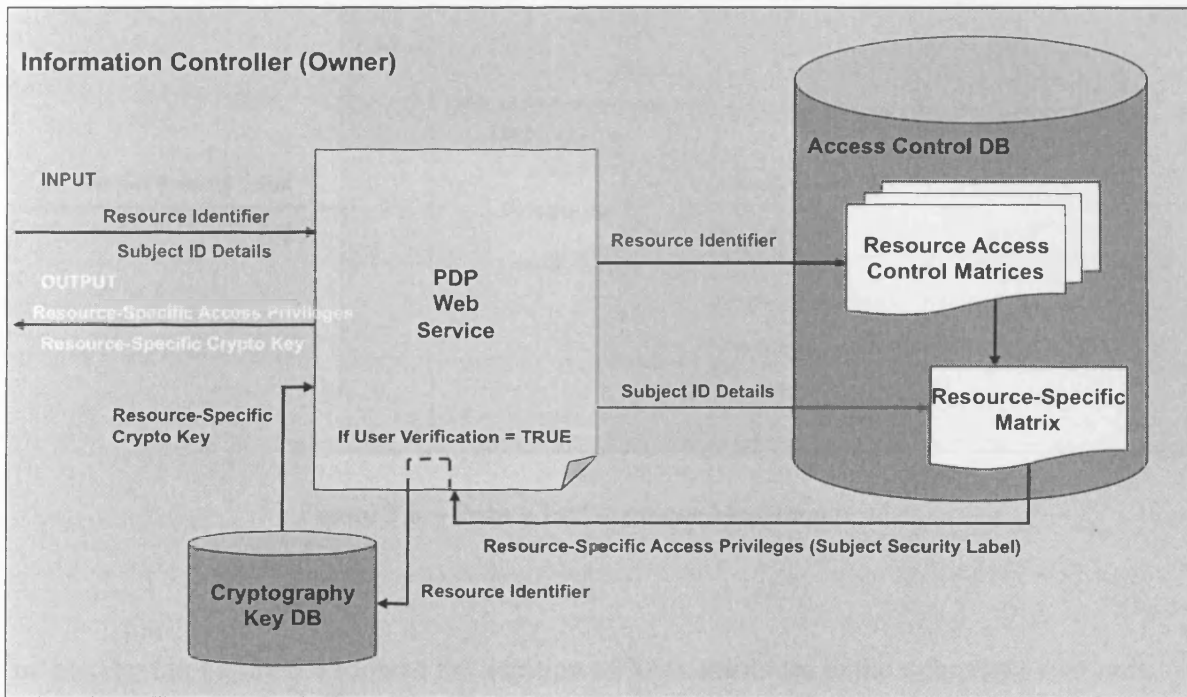


Figure 5.7 – Information Owner PDP

If the subject’s identity is found in the matrix, a *security label* is dynamically created for the subject. The subject’s security label contains the classification labels to which they have been granted access, and is made up of two parts: a *read element* and a *write element*. Each element contains a subset of the labels used to classify the resource, and defines the level of access the subject has been given to perform for that action (read and write). For example the *read* element could contain RED, AMBER and GREEN labels, giving full read access; while the *write* label may only contain the GREEN label, giving write access to only the unclassified content and content classified as GREEN.

The PDP service also locates the decryption key for the resource, using the resource identifier to extract the key from the table of encryption/decryption keys. The subject’s security label and the decryption key for the resource are returned to the policy enforcement mechanism across a secure channel. Figure 5.8 illustrates that the mechanism is then able to decrypt the resource and temporarily hold it in the memory of the machine it is running on.

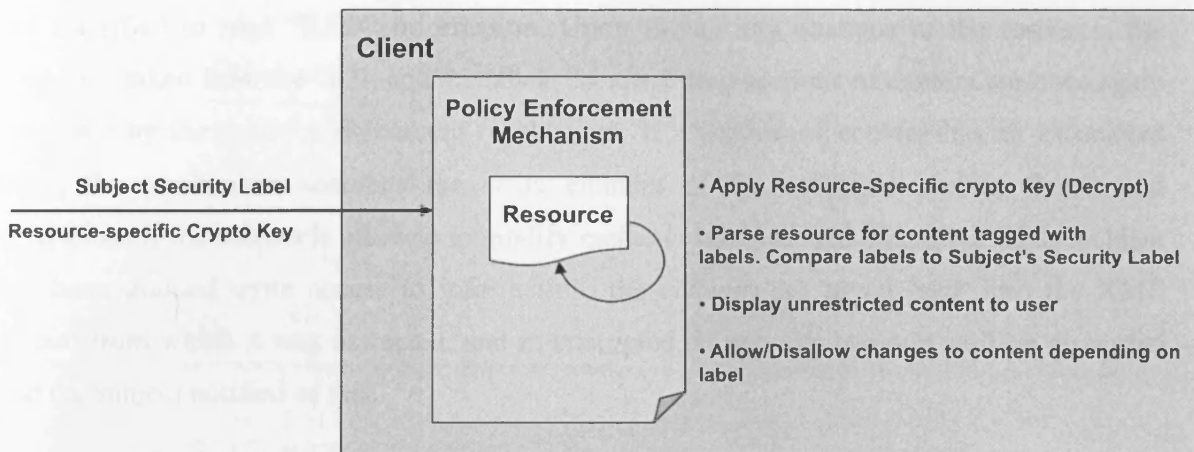


Figure 5.8 – Policy Enforcement Mechanism

The bold text in Figure 5.5 showed the addition of XML attributes to the <db:para> elements. Another advantage of XML is that it supports parsing tools, which allow elements to be searched for by name. The policy enforcement mechanism is able to scan through the resource held in the machine's memory, for elements with a specified name value. In this case, a search for the value "<db:para>" will locate the beginning of each paragraph in the document. Further XML searching capability allows the mechanism to extract all information between the <db:para> element and its associated closing element </db:para>, including the classification labels stored within the opening element.

If a label is present in the opening element, it defines the classification of the content encapsulated between that element and its closing element. When a label is found, the policy enforcement mechanism searches the subject's security label to determine if the subject has read or write access for content classified with that label, and enforces an access control decision. The mechanism effectively generates a new version of the information resource in the machine's memory. If the label is in the subject's security read label, the content is added to the new version. If not, the content will be omitted. Once the entire document has been parsed, the new version is displayed to the subject using the GUI, and the original document is closed. The subject can then read and edit the resource using the GUI. They are able to see the classification labels associated with the text they are reading, in order that they know the level of information they are reading and can handle it appropriately. For example, if they are reading "RED" information and they know they do not have "RED" write access, there is no point in them trying to modify it. Likewise, they should not show it to someone they know is

not classified to read “RED” information. Upon saving any changes to the resource, the content is taken from the GUI, and the labels encapsulating sections of content are once again inspected by the policy enforcement mechanism. If a section of content has an associated label, the mechanism searches the write element of the subject’s security label, and determines if the subject is allowed to modify content classified with that label. If the subject has been granted write access to information, the changes are saved back into the XML format from which it was extracted, and re-encrypted. If not, any changes will be discarded and the subject notified of this.

Access control restrictions, as defined in the access control matrix, are based on the information assurance requirements: confidentiality – meaning read access to information is restricted to certain people, and integrity – meaning write access to information is restricted to certain people, based on the identity attributes of the subject requesting the action. This may appear simple and obvious when considering access control models, such as Bell-LaPadula and Clark-Wilson, but it was not previously possible to take an information resource and apply these restrictions within the body of the information to selected sections of information, and then modify and enforce the restrictions at a later date, after information is shared outside of a controlled perimeter. This work has implemented the de-perimeterized access control formula as the enforcement controls are available outside the perimeter, and obeys the de-perimeterized linkage rule because there is permanent link between the policy enforcement point, the access control policy itself, and the resource owner.

5.3. Management of Information within the Application

All information modification takes place through the client side editing tool within the modified security model. It is understandable that many users will prefer to use their own editing tool, such as the proprietary Microsoft Office tools. In theory, this is not a problem; the conversion from proprietary format to XML is reversible. However there are limitations to doing this. By not using the GUI editor, the policy enforcement mechanism cannot be invoked; therefore, the information owner will lose the ability to enforce access control policy. This is because proprietary software does not currently support the ability to control whether or not the text is viewable and editable within a resource at paragraph level. The document is either read only or editable in its entirety, so the granularity over paragraph level control is lost. This is not a surprise, as it is one of the major issues highlighted in the

problem description of this thesis. The work has arrived at a requirement for more flexibility over information control, and to take the information back into the proprietary domain would defeat this aim. However, this scenario highlights the potential to bridge the gap between proprietary solutions and open standards based solutions, and illustrates one of the major failings in current information management controls.

The continuous link between information and its resource owner can be used to maintain a record of who exactly has access to information at any given time. This opens up the possibility to create logs of access control privileges granted and revoked, and resource access requests. This information could be useful in an audit of the access control system, should any breach of security occur, to find out who had access to the information when the breach occurred, following the suggestion of the Clark and Wilson access control model.

5.3.1. Policy Versioning

As information assurance requirements, legislation and regulation change over time, the labels used in an ICS to classify information, and the labelling decisions made on previously shared information, may also need to be modified to reflect the changes. This will involve revoking all existing access privileges to previously shared information that is affected by these changes, so that the new requirements can be fully enforced. This is done through policy versioning.

Each resource has its own access control matrix defining the identity credentials required to gain access to information held within the resource, based on the classification labels embedded within its body. Each resource has a globally unique identifier, which is bound to the access control matrix for the resource. The resource identifier is embedded as part of the body of the information, so that when a request for access is made, the policy decision point knows which access control matrix to use to make the access decision.

When a change of requirements occurs that affects a shared information resource, either to the labels used to classify the resource (the ICS), or to the assignment of labels within the resource (change of labelling required), existing information classification becomes invalid, and so all access needs to be revoked. This is done using the policy management interface by removing all access privileges, for all users, meaning that when somebody attempts to access the resource, they are notified that the policy has expired and that they need to obtain a new version of the resource. The important thing to note here is that the existing document now

becomes unusable, so the information is not at risk because of changes to classification requirements. Previously, there would have been no way to revoke access to shared information that had changed its classification.

This revocation of all access in light of a change in classification requirements involves policy management, which is not a trivial task, but can be built into the system as part of the information classification functionality. The first time information is labelled, it won't have an associated access control matrix or resource identifier. After the resource has been classified for the first time, by adding the security labels to the information, a resource identifier will be created and bound to the access control matrix for the resource. If a change in information classification requirements occurs, the current resource identifier can be marked as expired in its access control matrix. The matrix could be appended with a link to the new version of the resource, which can be returned to the requesting subject, allowing them to obtain a copy. The new version will be classified correctly and a subject will be able to access its content to the extent defined by the information owner.

Chapter 6 - Evaluation

To enhance current information security capability in support of more secure information sharing in collaborative distributed environments, the hypothesis of this research makes three claims, and the research has produced two formulae and a rule, based on an access control framework, in support of these claims. :

- i) security can be enforced at different levels of granularity within a document,

$$r_a = c_{ku} + \{=, >=, <=, >, <\} + c_{kd}, \text{ where } c_{kd} \in c_k$$

- ii) access control policy can be enforced outside the perimeter, no matter where it is stored within an Internet connected environment, and,

$$P_z = D + \{r_1 \dots r_n\} + E$$

- iii) access control policy can be modified and ii) is still applicable

There must exist a permanent link between a document d_x , e_b , $\{r_1 \dots r_n\}$, and P_z

The introductory chapters of this thesis have outlined a rationale and motivation for making these claims. The literature review of existing access control models and technology in Chapters 3 and 4 has shown that an implementation of these claims is lacking at present, and has drawn out the basic access control framework, from which two formulae and a rule have been defined to explain and address the limitations, and support these claims. The argument for the validity of these is in Section 4.3.2. Chapter 5 has detailed the implementation of a prototype application that was developed with an aim to test the feasibility of implementing the formulae and rule, and to enable finer-grained, remotely enforced, modifiable access control for information shared in collaborative distributed environments. In order to validate the feasibility of implementing the suggested formulae and rule in support of the claims of the hypothesis, an evaluation which consists of a set of testing scenarios and set of test scripts is used to test the prototype application does indeed implement the formulae and rules, and the enhancements do support these claims.

6.1. Testing Strategy

There are three key claims that the newly implemented technical solution must satisfy to support the hypothesis, which also relate to the risks identified in the three layer system threat

model. Namely: finer-grained access control; access control for information outside the perimeter; and modifiable access control policy after information has been shared. The evaluation of these claims follows a three step approach, evaluating each of the mechanisms in turn, to show the application makes these claims possible. The development of the formulae and rule has been argued within the framework that was set out in the first chapter to identify the problem, and used throughout to define and explain limitations of existing methods and tools. Therefore, if the argument is accepted, and the framework and formulae are logically correct, the formulae and rules theoretically solve the problems. The application has implemented them and if it can be tested to show the expected functionality exists, there is strong argument to support the claims of the hypothesis. This is why the evaluation approach has been developed this way.

Following evaluation, which determines whether the mechanisms support the hypothesis, a risk assessment will be performed on existing access control technology, and again on the advanced mechanisms, to determine if and how existing risks to information sharing in collaborative distributed environments have been mitigated, and if any new risks have been introduced by creating the new approach to access control enforcement.

The evaluation will use an information sharing scenario, to which the test scripts can be applied. The scenario will be based on the healthcare patient information sharing scenario identified in Chapter 1 as a motivation for the research. This is a particularly appropriate scenario as it includes personally identifiable information, something that a resource owner must retain appropriate control of in shared environments, under the Data Protection Act. It is also an information sharing scenario that is specifically cited by Anderson [And08], which he states has yet to be achieved.

The evaluation aim is to show that the prototype application that implements the new formulae, as documented in Chapter 5, works in such a way that the claims of the hypothesis can be supported. That is, to demonstrate the prototype application actually obeys the rules of the theoretical formulae and rule. The scenario will be used to do this. However, the evaluation approach does have its limitations. The scenario used is only a representative information sharing case. Other scenarios may have different security requirements and may produce different issues that may cause the new technology to fail. This is accepted as a limitation of the testing methodology.

6.1.1. Testing Scenario

The test scripts are based on a hypothetical testing environment and action-based scenario, using fictional users and data, but which is based on real-world access control requirements, actual organisational structure and a true-to-life information sharing scenario. The scenario is:

A patient presenting symptoms to their GP, is assessed, and diagnosed. A report is then written by the GP. If the symptoms present a case for further investigation, such as a painful lump beneath the skin, the GP refer the patient to a hospital for a scan. The presented symptoms, symptom duration, location and degree of pain it is causing will be added to the patient's Electronic Health Record (EHR). The hospital would be given access to the EHR to view the symptom detail, but not other information such as patient demographics, medical history or current medication. The hospital visit may result in a scan and an associated report. This will be added to the EHR. If required, the patient may be referred to a second hospital where they have a physics report produced. The second hospital would be given access to scan and initial symptoms, but not other information such as patient demographics, medical history or current medication. If a cancer is confirmed, the patient will be referred to a consultant oncologist who will write a prognosis report and write up a course of treatment, based on all the relevant information shared by the other institutions. The oncologist will need access to full medical history and current medication, so has a different access control requirement than the hospitals.

The actors in the scenario are also fictional but have roles based on real-world roles:

John Boxter is the GP at ThisTown GP Surgery

Pete Burnap is a clinician at ThisTown hospital performing the scan

Jason Ritchie is a clinician at ThatTown hospital performing the physics test

Ross Boone is a consultant oncologist at ThisTown cancer specialist clinic

The requirements for the information sharing scenario are that certain parts of the EHR need to be shared with different collaborating partners, based on their role within the collaboration.

The initial content of the EHR includes:

- Patient name and address

- Medical History
- Current Medication
- Past Lab Results
- Scanned Images

Not all of this content should be shared with every collaborator, as they do not need it all to conduct the duties required of their role. Access should not be assumed on inclusion in a VO, it should be given as required [PCC+06]. Appropriate security should limit the sharing of personal information. The less that is shared, the less likely there is that information will be leaked that can be used to affect the individual that it is relevant to the Data Protection Act (1998) [DPA98].

John Boxter is the GP. He will have full access to the EHR.

Pete Burnap will require access to part of the medical history, the part that contains the current symptoms the patient is presenting. But not the rest of the medical history, the current medication, or past lab results. He will add a new scanned image to the EHR, but not be able to see any of the other scanned images in the resource.

Jason Ritchie has the same access control requirements as Pete Burnap, and will have access to the scan that Pete added to the EHR.

Ross Boone will need access to the full medical history, current medication and the latest scanned images when accessing the EHR.

The technical enforcement mechanisms needed to facilitate these requirements mirror those identified in the threat model in Section 2.4, and reflect some of the issues discovered in the literature review of existing electronic information management. These are:

- The requirement to be able to control access and modification rights to content within a document, not just the entire resource. Different users should have different access rights depending on their role in the consortium,
- The requirement to be able to enforce the controls once the information has been distributed to collaborating project team members and is stored on remote, autonomous information systems, outside the control of the information owner. All users will be sent and given access to this document and be able to add to and modify

the contents. Access controls need to be applied to the information even after it has been shared outside the perimeter of the GP's protected network, and

- The requirement to be able to modify the controls at a later date from a centralised point. Once treatment of the patient ends, the collaborating parties will disperse and access to the EHR needs to be revoked by the GP to prevent any further use of the patient's data. Securing it in use for the purpose of treating the patient is appropriate. Letting the collaborators retain access once the goal of the collaboration is over is arguably unnecessary and inappropriate. It opens up the opportunity for information collation and use for secondary purposes.

Current access control technology cannot currently facilitate these requirements. This thesis hypothesises that these requirements can be made possible through enhanced access controls that implement the new formulae.

An example document to be access controlled is shown in Figure 6.1. This document is a sample EHR, containing some hypothetical content for the purposes of illustration of the concept.

6.1.2. Testing Environment

The mechanisms developed in support of the hypothesis claim to enable the aforementioned requirements to be applied to information, such as that contained in the exemplar document, which is to be shared in collaborative distributed environments. Thus, the environment in which testing is performed must replicate the sharing environment of a collaborative distributed system. To achieve this, four machines were setup on a wide area network replicating different users being on different networks and working on remote machines. The information owner (John Boxter) hosts the Policy Decision Point (PDP) Web Service, and holds the encryption keys and access control matrices for shared documents. He uses the mechanisms developed to define and apply the access control policy to the document being shared. Pete Burnap and Jason Ritchie are based on another Network replicating the Cardiff University internal network, and use the mechanisms to request access to the shared document, as does Ross Boone who is on another network replicating MyTime Consulting's internal network. The network architecture and links between remote users is illustrated in Figure 6.2. The environment has been designed in this way so that the mechanisms can be properly tested in a real-world environment. This will not only achieve the validation that the

mechanisms work correctly and enable an access control policy to be defined, modified and enforced, but may also pick up any environmental issues, such as network delays in accessing information, firewall blocks where requests between remote systems are blocked, and weaknesses in the security that arise from communication across the open, insecure Internet.

<p>Patient Details</p> <p>Joseph Bloggs 24 This Road This Street ThisPlace TH15 PLC</p> <p>Medical History</p> <p>1984 – Broken Fibia and Tibia 1990 – Chest Infection 1992 – Diagnosis of Asthma 1994 – Chronic Excema 1998 – Lower back pain 2000 – Broken Metatarsol 2010 – Painful lump on neck</p> <p>Current Medication</p> <p>Ventolin Inhaler</p> <p>Past Lab Results</p> <p>Screening for diabetes – Result: Negative</p> <p>Scanned Images</p> <p>Links to X-Ray image documents</p>

Figure 6.1 – Example Document (Unclassified)

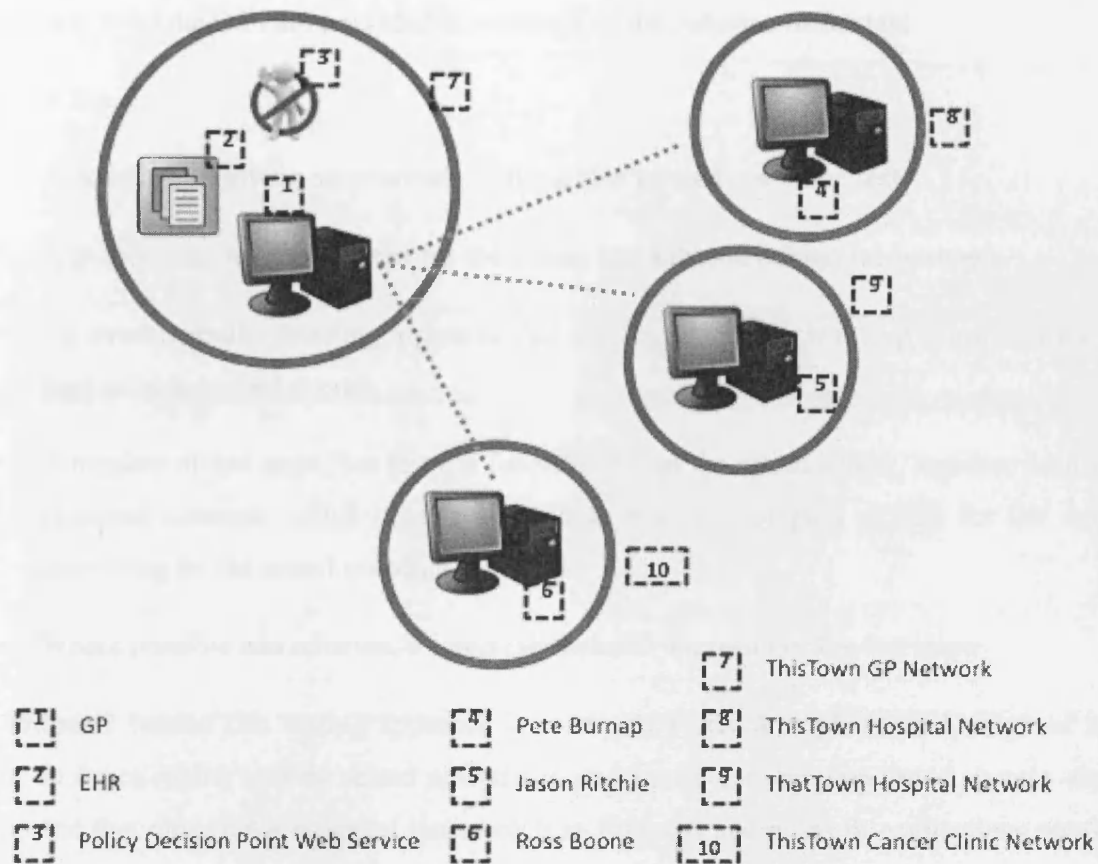


Figure 6.2 Testing Environment

6.2. Test Scripts

The test scripts detail tests to be applied to the mechanisms to validate their ability to support the advanced security requirements, and give the expected outcome of the test, should it be successful in supporting the claims of the hypothesis. To enable user interaction and to test the underlying mechanisms that have been developed, a lightweight Graphical User Interface (GUI) was developed to demonstrate the capability of the underlying mechanisms. The tool itself is lightweight, written in Java and will run on any platform. It does not even need to be installed, as it runs as a self-executing file that can be invoked across the Web. As the mechanisms perform access control definition and enforcement transparently to the user, it is difficult to capture evidence of them working. However, testing actions within the scripts make reference to the numbers in the testing environment diagram shown in Figure 6.2, so

that the action being carried out can be visualised to some extent and, where possible, screenshots from the GUI are provided as evidence of the outcome of the test.

Each test has:

- A description, giving an overview of the action carried out in the test
- A purpose, giving more detail for the action and a reason behind its existence
- An overall result, detailing a pass or fail for the test. Every test step must pass for a pass to be achieved overall
- A number of test steps that test the functionality of the tested action, together with an expected outcome which creates a result in the form of pass or fail for the step, depending on the actual outcome.
- Where possible and relevant, a screen shot shows the result of the test steps

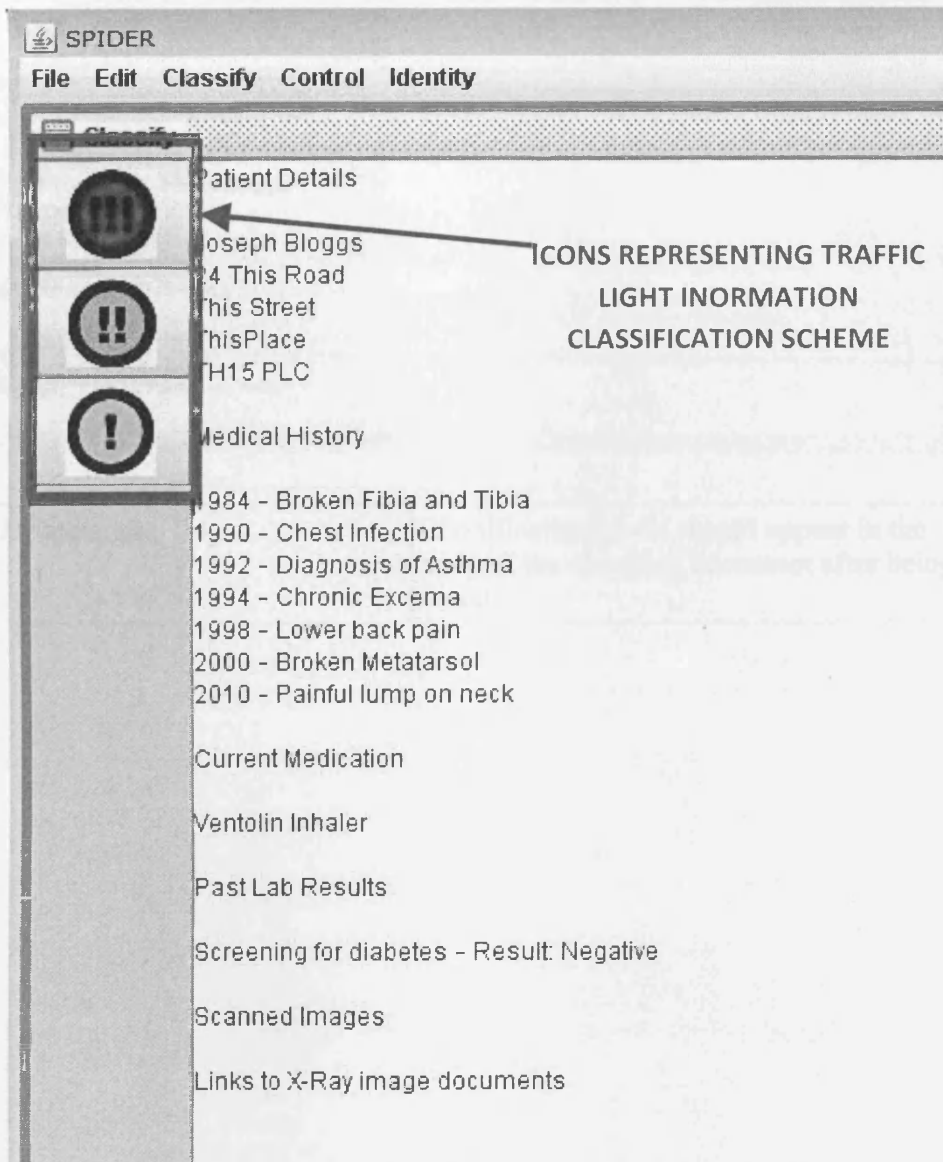
The rationale behind this testing approach is to create a walkthrough of each stage of an action so functionality can be tested and errors and issues can be pinpointed. It was also anticipated that other environmental issues such as firewalls and network connections would become evident during the step-by-step process. At the end of the test process, each action is fully tested and validated for its anticipated functionality.

6.2.1. Test Phase 1 – Advanced granularity of control over information.

This test demonstrates that it is possible to drill down into the body of an information resource and apply security requirements within the content of the resource - thus overcoming the limitation of file-level classification in proprietary information. The GUI is used, together with the traffic light information classification scheme, defined in Section 5.1.1, to invoke the policy definition mechanism, and apply this level of control to a proprietary document format. It is then used to define access privileges to the labels embedded in this specific document, for collaborating users. As Microsoft Word is arguably the most popular document editing tool at present, in that most people in a collaborative environment share and edit documents using Microsoft Word, it was decided that a Microsoft Word 2003 document should be used as the test case document. The DocVert Web Service [DV] is used to convert the Word Document to raw XML prior to being used in the example.

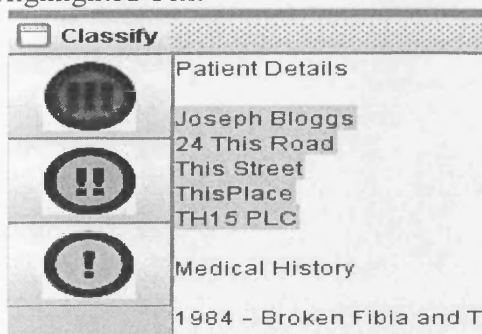
In relation to the testing environment diagram in Figure 6.2, this test is being carried out within the GP's internal network, marked as number 7 in the diagram. There is no network functionality testing and no application of access control policy. This is purely designed to test the functionality of access control labelling.

Test #	1	
Description	Apply access control metadata to a proprietary document	
Purpose	To enable part of the access control policy to exist within the body of an information resource so that it can be used to enforce access control remotely.	
Overall Result	Pass	
Steps	Expected Outcome	Step Result
1 – Run the prototype application GUI.	The main application window should appear.	P
2 – Use the GUI to load a document into the editor	'Open' dialog should appear allowing user to select a file. Text should appear in the editor pane after a file is selected.	P





3 – Highlight sections of text and click an information classification label to apply the label to the document	Label should appear at the beginning and the end of the highlighted section.	P
---	--	---

Highlighted Text



Classified Text

Classify	
	Patient Details [*] BEGIN Red] Joseph Bloggs 24 This Road This Street ThisPlace TH15 PLC [*] END Red]
	Medical History 1004 - Broken Fibia and Tibia

4 – Save the document

Classification labels should appear in the body of the classified document after being saved

P


```

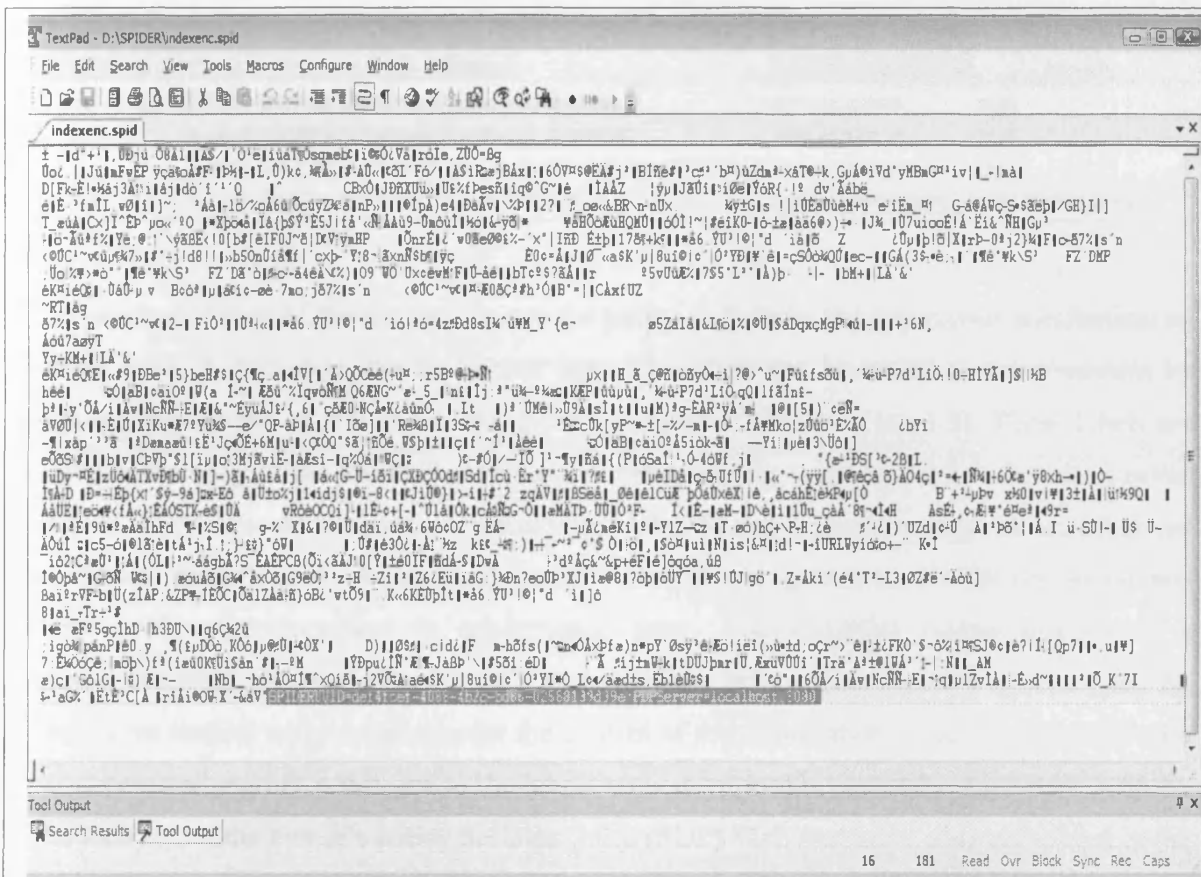
<?xml version="1.0" ?><db:book xmlns:db="http://docbook.org/ns/docbook"
xmlns:html="http://www.w3.org/1999/xhtml" xml:lang="en" version="5.0">
<db:preface>
<db:para label="">Patient Details</db:para>
<db:para label=""></db:para>
<db:para label="Red">Joseph Bloggs</db:para>
<db:para label="Red">24 This Road</db:para>
<db:para label="Red">This Street</db:para>
<db:para label="Red">ThisPlace</db:para>
<db:para label="Red">TH15 PLC</db:para>
<db:para label=""></db:para>
<db:para label=""></db:para>
<db:para label="">Medical History</db:para>
<db:para label=""></db:para>
<db:para label="Red">1984 ^ Broken Fibia and Tibia</db:para>
<db:para label="Red">1990 ^ Chest Infection</db:para>
<db:para label="Red">1992 ^ Diagnosis of Asthma</db:para>
<db:para label="Red">1994 ^ Chronic Excema</db:para>
<db:para label="Red">1998 ^ Lower back pain</db:para>
<db:para label="Red">2000 ^ Broken Metatarsol</db:para>
<db:para label=""></db:para>
<db:para label="Amber">2010 ^ Painful lump on neck</db:para>
<db:para label=""></db:para>
<db:para label=""></db:para>
<db:para label="">Current Medication</db:para>
<db:para label=""></db:para>
<db:para label="Red">Ventolin Inhaler</db:para>
<db:para label=""></db:para>
<db:para label=""></db:para>
<db:para label="">Past Lab Results</db:para>
<db:para label=""></db:para>
<db:para label="Red">Screening for diabetes ^ Result: Negative</db:para>
<db:para label=""></db:para>
<db:para label=""></db:para>
<db:para label="">Scanned Images</db:para>
<db:para label=""></db:para>
<db:para label="Amber">Links to X-Ray image documents</db:para>
<db:para label=""></db:para>
</db:preface>
</db:book>

```

5 – Encrypt the document

Document should be encrypted on saving.
The PDP location and Document ID
should be appended to the bottom of the
file and remain unencrypted

P

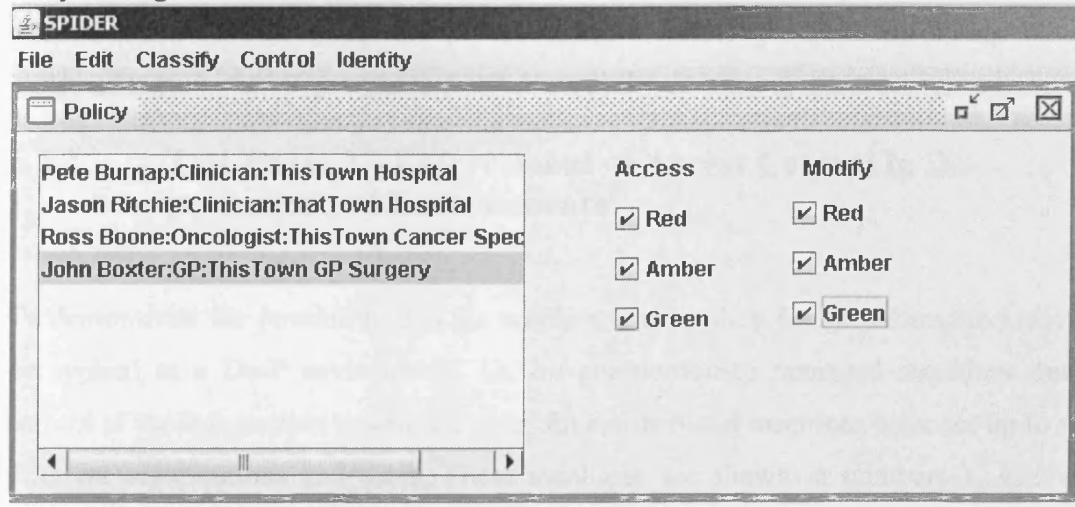


6 – Define access control policy for the labels embedded within the document

The labels are now embedded within the document. These will travel with the document and relate to a centralised access control matrix, defining who has access to those labels

P

Policy Management Window within GUI



Relating Access Control Matrix in MS Access

Users			
ID	User	Access	Modify
2	Pete Burnap:Clinician:ThisTown Hospital	amber:green	null
3	Jason Ritchie:Clinician:ThatTown Hospital	amber:green	null
4	Ross Boone:Oncologist:ThisTown Cancer Specialist Unit	red:amber:green	null
5	John Boxter:GP:ThisTown GP Surgery	red:amber:green	red:amber:green

The passing of each of the test steps gives the policy definition and application mechanism an overall pass. A document can be opened (step 2). Labels can be added to the document by highlighting chunks of text and clicking the appropriate label icon (step 3). These labels are stored in the body of the information resource, transparently to the user when the file is saved (step 4). The whole document is then encrypted (step 5) and is protected against unauthorised access and modification. A unique document identifier is generated for the document and stored within the document in unencrypted form. The identifier relates directly to a document-specific access control matrix stored on the information owner's system (step 6). The access control table remains under the control of the information owner, and defines who has access and modify privileges to the labels embedded in this particular document (step 6). The location of the owner's policy decision point (PDP) Web Service is also embedded in the document, in unencrypted form (step 5). The policy enforcement mechanisms (which are tested next) can extract the document identifier and PDP location and send access requests to the PDP along with the document identifier, so that the PDP service knows which document a user is requesting access to and can query the appropriate access control table. At this point the document can now be distributed with security labels embedded and encrypted along with the rest of the content. The information is now unreadable until the policy enforcement mechanism is used to request access and decrypt the document.

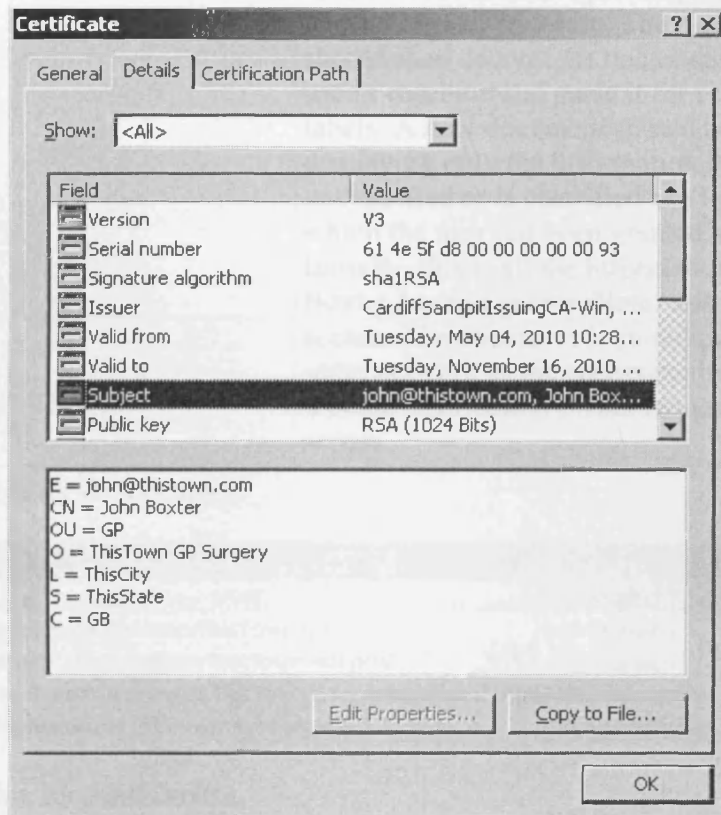
6.2.2. Test Phase 2 – Enforcement of Access Control in De-perimeterized Environments

To demonstrate the possibility that the access control policy for an information resource can be applied in a De-P environment, i.e. on autonomously managed machines outside the control of the information resource owner, four distributed machines were set up to represent different organisations and users. These machines are shown in numbers 1, 4, 5 and 6 in Figure 6.2. A different identity and role was created for a user on each machine based on the identities defined in the testing scenario.

In the scenario described, the now encrypted document (numbered 2 in Figure 6.2) is sent to each user to be accessed on their local machines. At this point the information owner would previously be giving up all control of their information. This is a limitation of existing access control technology and the perimeterized security model. To advance current security models, the policy enforcement mechanism developed in support of the claims in this thesis, together with the information classification labels embedded within the information resource, as achieved in test 1, are used to maintain some control over information after it has been shared, by locally enforcing the (remote) access control policy for the distributed resource. A user wishing to access the document must use the client mode of the GUI to open and view it, mandating enforcement of application-based controls, based on the Clark-Wilson model and existing DRM approaches, and in doing so, the GUI acts as a proxy to invoke the underlying mechanisms and request access remotely to the PDP and thus open the document to view.

This test is designed to check the functionality of remote policy enforcement. When the document is sent to Pete Burnap, Jason Ritchie and Ross Boone, it leaves John Boxter's network perimeter and enters the autonomously managed network perimeters of the hospitals and the cancer clinic. John Boxter cannot have any control within these perimeters unless he has a remote service enforcing policy on his behalf. This is the purpose of the policy enforcement mechanism developed in support of making de-perimeterized access control a possibility.

Test #	2	
Description	Enforce access control policy on a remote endpoint outside of the control of the information owner	
Purpose	To enable access control policy defined by the information owner to be enforced when the information resource is stored on information systems outside their control	
Overall Result	Pass	
Steps	Expected Outcome	Step Result
1 – Run the application.	The main application window should appear.	P
2 – Select an identity to use when accessing the document. First use John Boxter from his local machine, pictured as number 1 in Fig 6.2	'Open' dialog should appear allowing user to select a Digital Certificate to use as identity credentials. Identity credentials should load into the GUI when a certificate has been selected	P
User Certificate		



Identity Credentials loaded into GUI



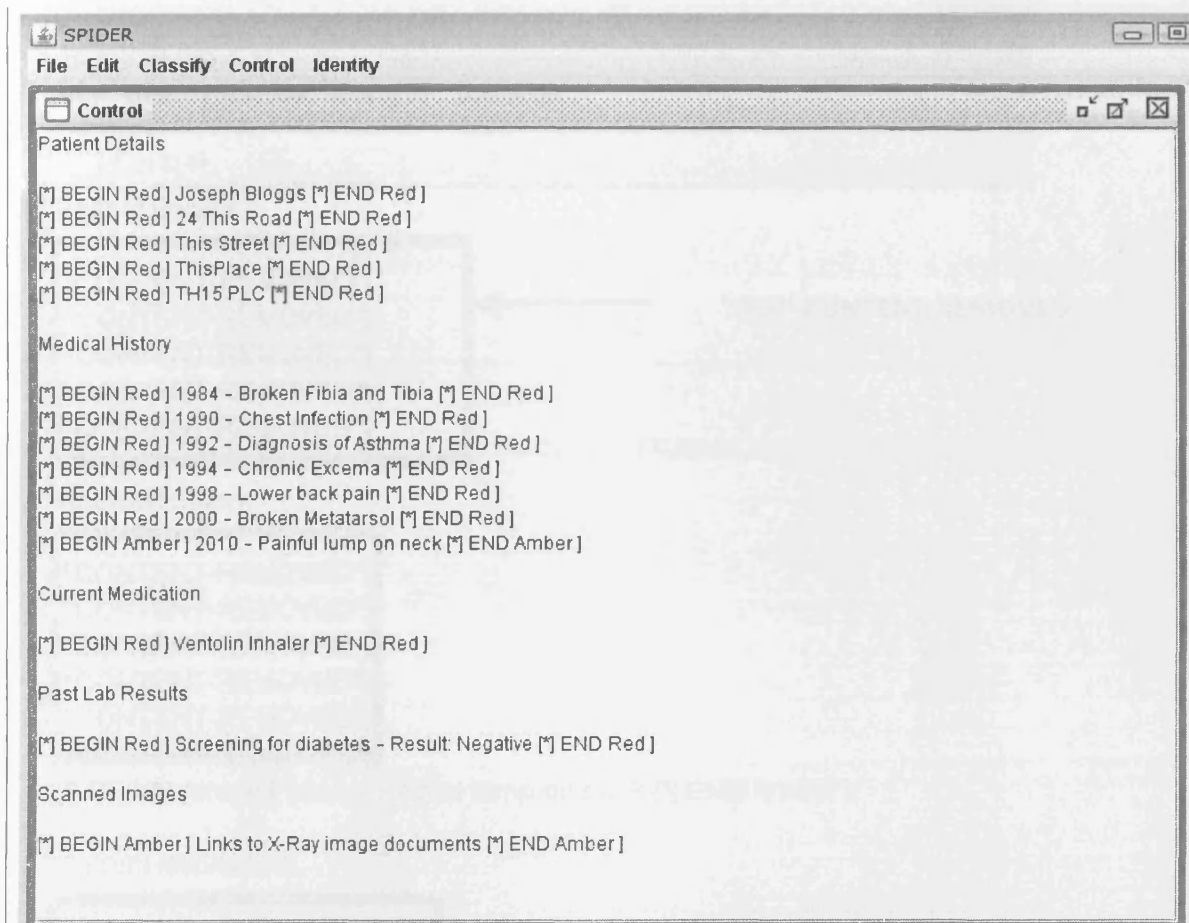
3 – Load a document into the editor	‘Open’ dialog should appear allowing user to select a file. Text should appear in the editor pane after a file is selected. The underlying policy enforcement mechanism should create an access request to the PDP for this particular document, and should	P
-------------------------------------	---	---

receive a set of access privileges and a decryption key in return. The mechanisms should then decrypt the document on the user's machine and parse it for security labels. A new document should be created displaying only the information that is unclassified or is classified at a level to which the user has been granted access. Initially, this is all the information as John Boxter has full access. Note: this is local access. The document is stored on the same network as the access control table as it is the information owner requesting access

Access control table for the document

Users			
ID	User	Access	Modify
2	Pete Burnap:Clinician:ThisTown Hospital	amber:green	null
3	Jason Ritchie:Clinician:ThatTown Hospital	amber:green	null
4	Ross Boone:Oncologist:ThisTown Cancer Specialist Unit	red:amber:green	null
5	John Boxter:GP:ThisTown GP Surgery	red:amber:green	red:amber:green

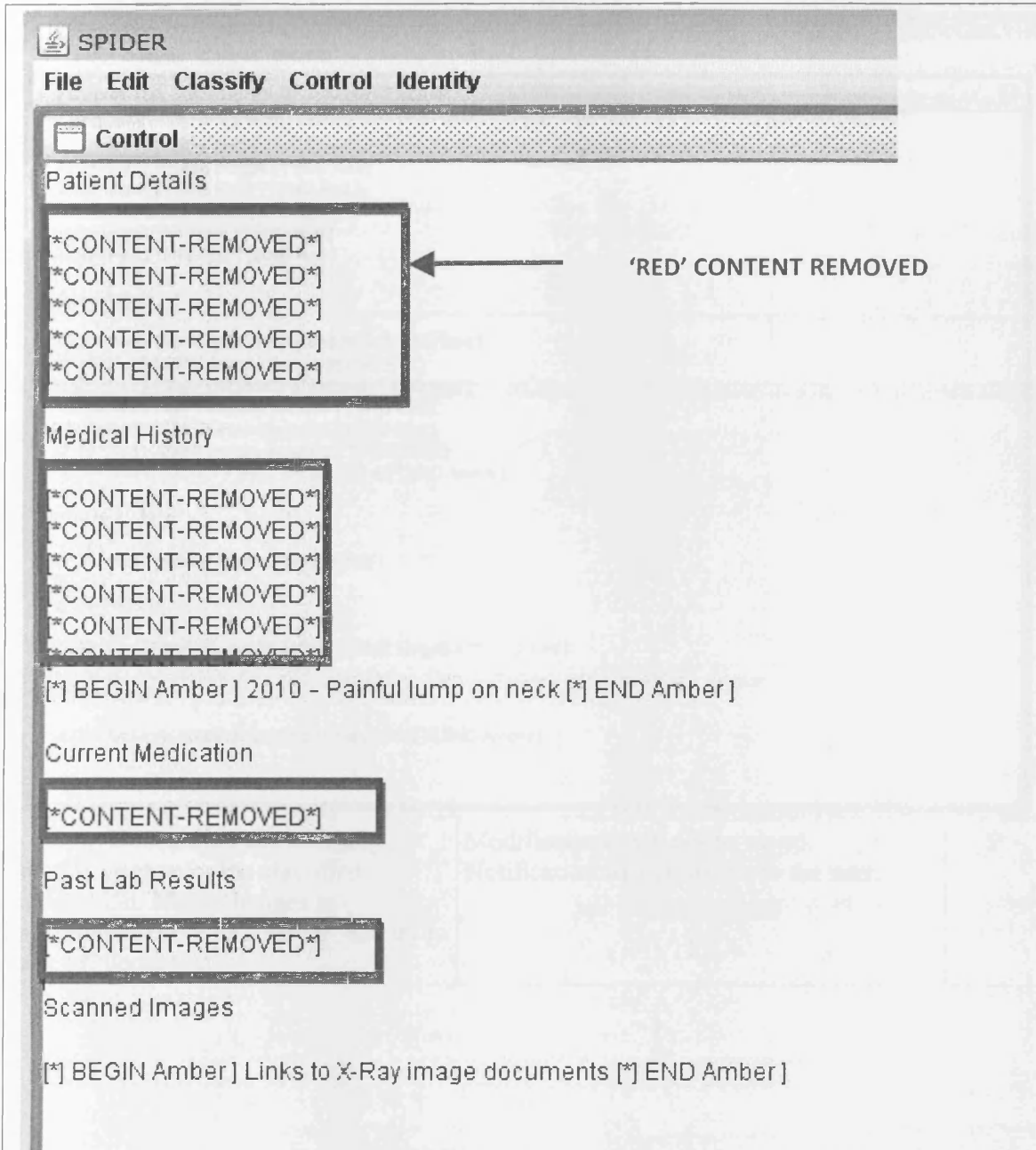
View of information for John Boxter



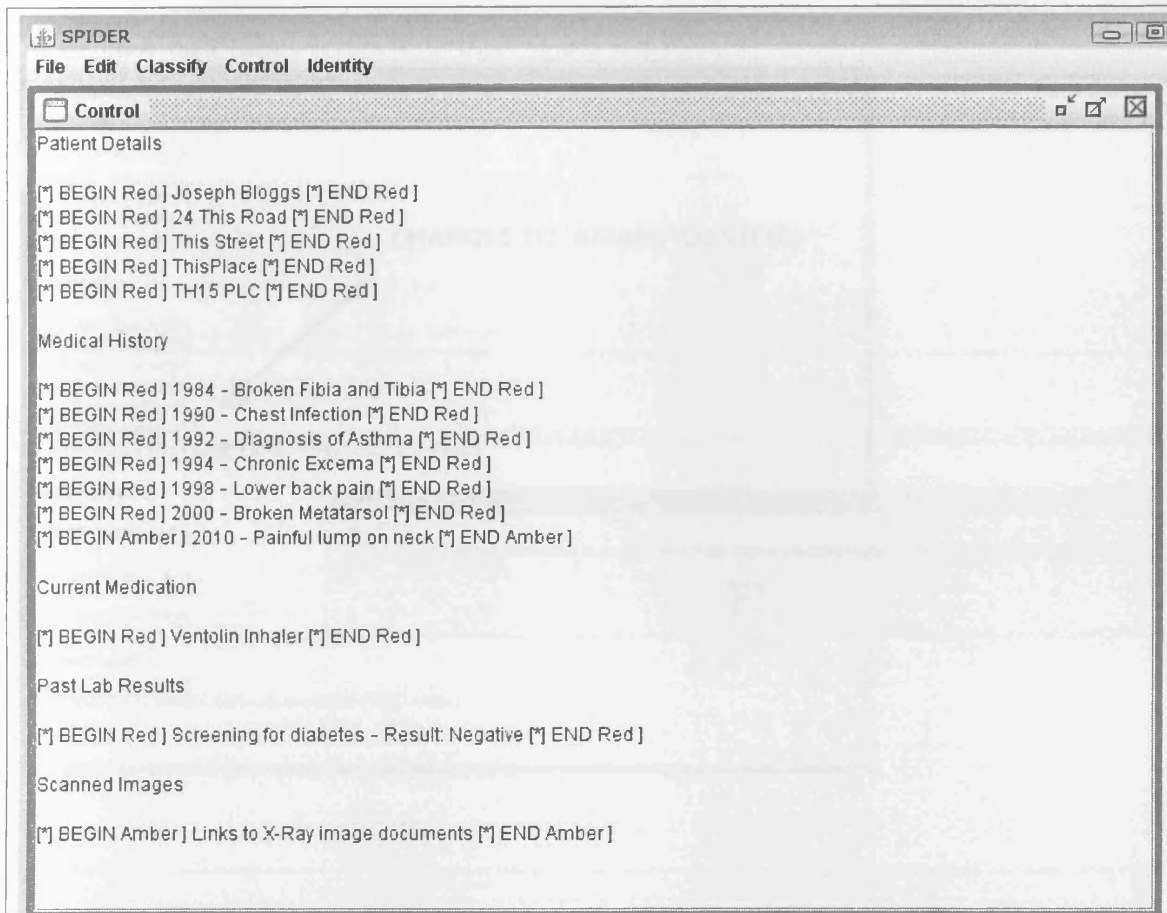
4 – Access the document from a different machine on another network as a different user identity. Use the identity of Jason Ritchie from his local machine, pictured as number 5 in Fig 6.2

The view of information should be changed. Jason Ritchie should not be able to view any information classified as 'red'. Note: this request happens between firewalled networks so, if successful, this also proves that the mechanism communication can navigate firewalls. It will also highlight any delays to access through network delay

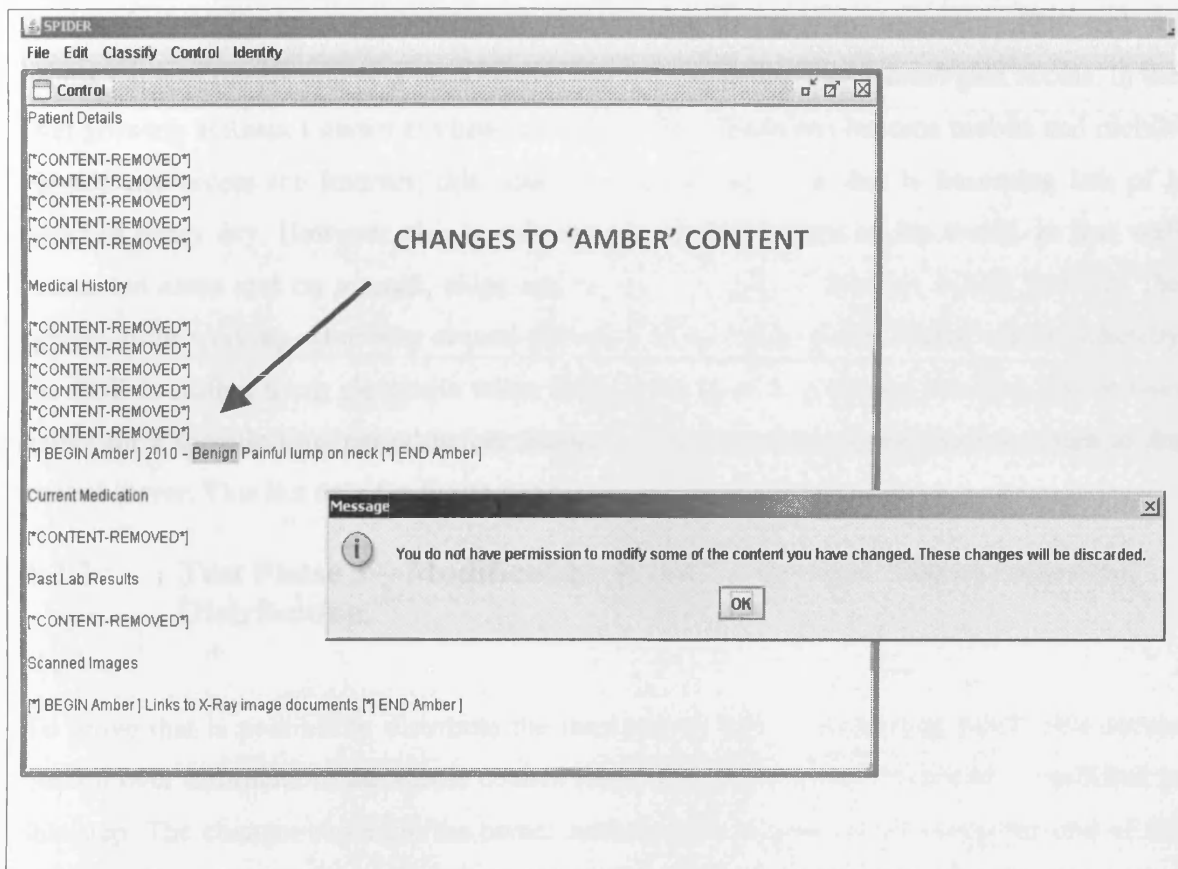
P



<p>5 - Access the document from a different machine on another network as a different user identity. Use the identity of Ross Boone on his local machine, pictured as number 6 in Fig 6.2.</p>	<p>The view of information should be changed. Ross Boone should be able to see all information</p>	<p>P</p>
--	--	----------



<p>5 – Ross Boone does not have any ‘modify’ rights for the classified information. Make changes to information classified ‘amber’ and try to save the document.</p>	<p>Modifications will not be saved. Notification will be shown to the user.</p>	<p>P</p>
--	---	----------



The passing of this test demonstrates that access control enforcement for the shared document is achievable between and across remote networks where the machines on those networks are running the prototype mechanisms. Firewalls were present on all machines and posed no problem. However, the network port listening for incoming requests was port 8080 which is the standard port used in Apache Tomcat, the web server used to host the PDP web service. This port is configured within many firewalls to allow incoming requests from the Internet. If the port is changed to something else such as 1234, the firewall must be configured to accept requests on that port. If it is not, access will be blocked. This is not a limitation as much as a setup requirement.

The machines were tested on Wide Area Networks and no time delay was evident when sending and receiving access requests and responses to remote servers. The amount of data required to be sent each way is very small and as such causes minimal delay. With regard to scalability, you may expect to see a slightly longer delay as the number of shared resources and number of sharing users rises, as there are more potential access control tables to search, and more users to search through.

One issue that is evident is that if no connection can be made to the remote PDP with an access request, the document is inaccessible and the requesting user cannot gain access. In the ever growing ambient Internet environment where Broadband has become mobile and mobile phones can access the Internet; this could be seen as an issue that is becoming less of a problem every day. However, this is only the case in some parts of the world. In less well connected areas and on aircraft, ships and so on, the lack of Internet access prevents the system from working. One way around this may be to produce time-based tokens whereby the PDP is shifted to an electronic token that can be sent to a remote machine and remain active for a specific time period before becoming inactive and requests need to return to the central server. This is a case for future work.

6.2.3. Test Phase 3 – Modification of Access Control Policy following Distribution.

To prove that is possible to distribute the information while maintaining modifiable access control over information, the access control table under John Boxter’s control is modified in this step. The changes represent the owner revisiting the document following the end of the collaborative effort and reviewing the previously defined access controls. The owner can modify the privileges in their access control table so that some of the content is more strictly controlled, and some of the content is less strictly controlled. The changes are representative of the same real-world activity that the fictional test scenario is based on:

John Boxter’s access remains the same as he is the information owner and retains full access.

Pete Burnap, Jason Ritchie and Ross Boone can no longer see any part of the classified patient record as they no longer need it once the collaboration is over.

This test is designed to test the ability to change the details in an access control table and for the enforcement mechanism to produce a different document view for users, based on these changes.

Test #	3
Description	Modify access control table form a central point and see the changes enforced at remote endpoints outside of the control of the information owner

Purpose	To enable access control policy defined by the information owner to be modified after the information has been shared, and continue to be enforced when the information resource is stored on information systems outside their control
----------------	---

Overall Result	Pass
-----------------------	------

Steps	Expected Outcome	Step Result
1 – Run the application.	The main application window should appear.	P
2 – Make changes to the access control matrix representative of the changes detailed above.	Access control matrix will have a different set of access controls for this document.	P

Access Control matrix before changes

Users			
ID	User	Access	Modify
2	Pete Burnap:Clinician:ThisTown Hospital	amber:green	null
3	Jason Ritchie:Clinician:ThatTown Hospital	amber:green	null
4	Ross Boone:Oncologist:ThisTown Cancer Specialist Unit	red:amber:green	null
5	John Boaxter:GP:ThisTown GP Surgery	red:amber:green	red:amber:green

Access Control matrix after changes

Users			
ID	User	Access	Modify
2	Pete Burnap:Clinician:ThisTown Hospital	null	null
3	Jason Ritchie:Clinician:ThatTown Hospital	null	null
4	Ross Boone:Oncologist:ThisTown Cancer Specialist Unit	null	null
5	John Boaxter:GP:ThisTown GP Surgery	red:amber:green	red:amber:green

3 – Select an identity to use when accessing the document. Use the identity of Jason Ritchie from his local machine, pictured as number 5 in Fig 6.2	‘Open’ dialog should appear allowing user to select a Digital Certificate to use as identity credentials. Identity credentials should load into the GUI when a certificate has been selected	P (see test 2.2)
--	--	---------------------

4 – Load a document into the editor	As 2.3. Policy should be enforced, however, the new changes to the access control matrix should be reflected when the policy is enforced.	P
-------------------------------------	---	---

Previous view of information for Jason Ritchie

[*CONTENT-REMOVED*]
[*CONTENT-REMOVED*]
[*CONTENT-REMOVED*]
[*CONTENT-REMOVED*]
[*CONTENT-REMOVED*]

[*] BEGIN Amber] 2010 - Painful lump on neck [*] END Amber]

Current Medication

[*CONTENT-REMOVED*]

'AMBER' CONTENT SHOWN

Past Lab Results

[*CONTENT-REMOVED*]

Scanned Images

[*] BEGIN Amber] Links to X-Ray image documents [*] END Amber]

New view with access control table changes (removal of of 'amber' access)

Medical History

CONTENT-REMOVED*]
CONTENT-REMOVED*]
CONTENT-REMOVED*]
CONTENT-REMOVED*]
CONTENT-REMOVED*]
CONTENT-REMOVED*]

CONTENT-REMOVED*]

'AMBER' CONTENT REMOVED

Current Medication

CONTENT-REMOVED*]

Past Lab Results

CONTENT-REMOVED*]

Scanned Images

CONTENT-REMOVED*]

The passing of this test proves that it is possible for the information owner to change the previously defined access privileges for a collaborative partner, after they have shared information with them, and see the changes enforced next time the partner accesses the document. Previously, once a document had been shared, all control over it was lost. Now, with the development of a de-perimeterized access control enforcement mechanism that links to a centrally managed policy decision point, any changes to access control requirements can be locally modified and remotely enforced with immediate effect.

The passing of all three tests demonstrates that the claims made in the hypothesis are valid and possible. It also demonstrates a working prototype of a system that supports the requirements of the system threat model defined in Section 2.4. One limitation that is evident in relation to the third risk of the system threat model is that the risk is actually defined as collaborating users not being able to control access to their own content in a collaboratively developed resource. This prototype enables information to be classified by its owner and continuously controlled in a shared, De-P environment, which mitigates the risk to a large extent. However, ideally, each collaborator should control access to their *own* information. This means that when they access a shared document and add content to it, they should be able to use the same mechanisms to apply classification labels and relative controls to the content they have added. This functionality is currently not present. In theory, this would mean multiple resource identifiers and multiple PDP locations to be embedded in a single document. Each time access is requested, the policy enforcement mechanism would have to request access to each and every PDP stored in the resource. This is something that will be considered in future work.

6.3. Position to Existing Technology

The rationale behind the development of the advanced security mechanisms was to advance the security available to distributed collaborators through existing access control technologies. The analysis of existing access control technology shows there are already several very well development systems that deal with identity management and access control policy in distributed environments. The lack of granularity, and as a result, lack of ability to modify access control policy within a finer-grained solution is evident in current technology. This thesis aimed to prove that, with the approach developed through the research, it is

possible to achieve this using open standards and software. The evaluation chapter has presented the evidence to demonstrate this is possible.

It is envisaged that the advanced access control functionality enabled by the mechanisms could be integrated with existing technology in one of three ways, explained below and using Figure 6.3:

Scenario A: As a separate entity that interfaces with an existing technology but remains a standalone implementation. This would be the case where access to application code is not possible, but developing plug-ins to enable an interface is possible. This may be the case if it were implemented with Microsoft Word.

Scenario B: As a semi-integrated entity that is built in to an existing technology to some extent, but where part of the solution is not integrated and remains a standalone entity. This would be the case when access to application code is possible, but the application does not support some of the required functionality, such as database connectivity or web based connectivity.

Scenario C: As a fully integrated entity that is completely built into an existing technology. All database connectivity and communication, text editing and access control policy development takes place inside the technology through the interface within an existing application. This will be the most difficult to achieve, but is certainly possible with open source and open standards software.

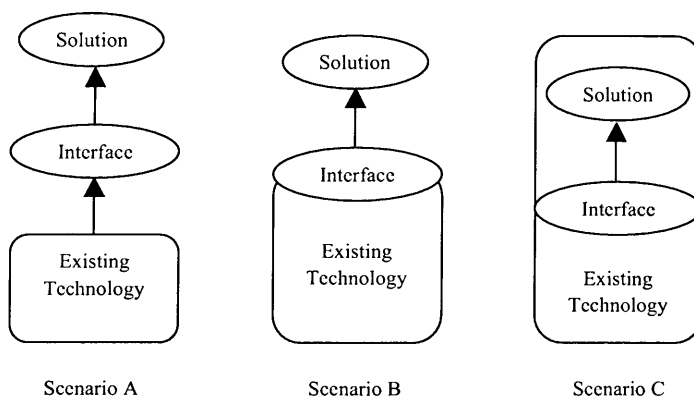


Figure 6.3 – Visualisation of Solution Integration with Existing Tools

6.4. Risk Assessment

The threat model defined in Section 2.4, from which the requirements of the mechanism developed in support of the hypothesis were derived, was developed using a qualitative risk assessment of the literature review covering current methods of electronic information management. The most pertinent threats were drawn into the system threat model.

Having evaluated existing access control technology through the literature review in Chapter 4, which discovered that current technology was largely perimeter based; and having developed a set of mechanism that provide advanced access control for de-perimeterized environments, it is necessary to evaluate the existing risk to information secured within the perimeter and shared in collaborative distributed environments, in order to define if and how these risks have been mitigated in the de-perimeterized approach presented in this thesis. This is documented in Table 6.1. Following that, it is also essential that any new risk to information outside the perimeter is also evaluated, to define limits on the security afforded to information shared in this way and secured using the suggested approach. This is captured in Table 6.2.






Asset	Vulnerability	Threat Agent	Recommended Response	Mitigated in Solution?	How Mitigated
Information stored within network perimeter	Unauthorised access through firewall hack	Internal or external malicious user	Encrypt in situ		Tool encrypts all new information by default, existing information after classification
	Authorised access but loss of control if information is moved/stored outside the perimeter	Any authorised user	Prevent data moving outside the perimeter or protect it if it does move.		Information allowed to move outside perimeter, no more loss of control due to link to central policy decision point and de-perimeterized policy enforcement point
	“Analog Hole” – People being able to read/copy/photograph information	Any user that gets hold of the data	There is nothing you can do about this.		Once information has been viewed, there is no way of controlling that information. It can be memorised, copied out by hand, photographed and so on.
Information shared outside the perimeter	Outside of perimeter of access control	Any user that gets hold of the data	Encrypt outside the perimeter		Information shared outside the perimeter must first be classified using the tool, which encrypts it before sharing
Highly sensitive content in an information resource	Confidentiality/Integrity breach. Data exposure	Any user that gets hold of the data	Classify and restrict access to highly sensitive data		Tool allows information within a resource to be classified according to its security requirement in accordance with ISO 27001:2005

Table 6.1 - Risk Assessment – Perimeterized Access Control (with current controls)



Vulnerability Mitigated



Unable to mitigate Vulnerability

To summarise, the recommended response to the vulnerabilities in the perimeterized access control model is largely focussed around the use of encryption and information classification to enable maximum confidentiality and integrity for information stored within the perimeter, and when shared outside the perimeter. Unsurprisingly this mirrors the suggestion of ISO 27001:2005, which suggests the classification of information, and the Data Protection Act 1998 which requires “appropriate security” measures to be taken, to which HMRC and ONS have responded with a complete lockdown of unencrypted data being taken outside of the perimeter. The mechanisms developed in support of this thesis support a shift to a de-perimeterized model, where the vulnerabilities identified in the perimeterized model can be mitigated, providing “appropriate security” through the encryption and continuous control over information shared outside the perimeter. Most of the risks to information shared in collaborative distributed environments and secured using the perimeterized approach are mitigated through the mechanisms developed in support of this thesis. One issue that cannot be solved is the ‘Analog Hole’ issue. This is the problem where text must ultimately be displayed to a user such that they can read and process the information. Once a person has read something, they can memorise it and reproduce it. They can also photograph it; copy it down and screen dump the content. There is currently no way of preventing this in either approach.

While the mechanisms provide the ability to share information outside the perimeter of control, they also present new vulnerabilities, as highlighted in Table 6.2. The major vulnerability introduced when allowing information to move outside the secured perimeter comes with the enforcement of de-perimeterized controls. The information shared remains encrypted until such a time as a request is made, through the mechanism developed, to the centralised point of policy decision. This communication and the response from the server containing the access control privileges for that user and the decryption key for the information is secured using an encrypted communication link, thus protecting the decryption key and access privileges. The mechanisms are then used, along with the decryption key, to decrypt the information on the user’s machines; parse the information for information security labels; and enforce the access controls by removing confidential information to which the user does not have access privileges, and marking the integrity sensitive information so that it can only be modified (saved after modification by the user) if

they have the appropriate privileges. All of this is done in the memory of the machine from which access is requested and on which the information resides. At some point, after decryption, the information, access privileges, classification labels and decryption key will be held in clear text in the computer's memory. If a malicious user was able to capture memory content at this point, or stream it into a new file, the information could be leaked. Alongside screen-scraping, which cannot be avoided completely due to the fact that information is displayed on the screen for the user to read, this is the major vulnerability of the modified architecture for access control. The vulnerability really comes from the machine being used to access the information being outside the information owner's control. Although the access control enforcement mechanism acts as a remote agent on behalf of the information owner to enforce policy, the memory of the machine is accessible to the person requesting access as they have physical access to the machine. A threat to this vulnerability is much less likely to occur in a perimeterized model because the memory of the machine is not so readily accessible to the person requesting access because they have no physical access to the machine.




Asset	Vulnerability	Threat Agent	Recommended Response	Addressed by Tool?
Information shared outside the perimeter	Unauthorised access through memory hack	Internal or external malicious user	Use memory curtaining to detect hack and wipe data	
Decryption key and Access Privileges in transit	Key or Privileges capture through sniffing the connection to the server	Hacker	Encrypt client-server communication	
Encryption Algorithm/Key	Cracking of encryption key and/or algorithm	Hacker	Use strongest possible algorithm and suitably large key	

Table 6.2. Risk Assessment – De-Perimeterized Access Control (with new controls)

This vulnerability could be overcome by using Trusted Computing technology. Trusted Computing allows what is known as Memory Curtaining, which prevents any hardware or software, even the operating system itself, from accessing specific sections of memory. This could prevent malicious users capturing knowledge from the memory of a machine by wiping the information if memory tampering is detected. While this goes some way to mitigating the vulnerability of memory attacks, it also requires every user using the de-perimeterized approach to have a Trusted Computing chip in their machines in order to make the approach more secure. Trusted Computing chips are becoming more readily available within machines but the whole ethos of the de-perimeterized approach is that information can be shared with anyone, regardless of the operating system, computing platforms or hardware specifics of local machines. To mandate the use of Trusted Computing chips would dramatically reduce the number of users able to receive this shared information. This means that this vulnerability is an ongoing one. There may be a point in time in the future where Trusted Computing chips are built in to every computer, at which time the de-perimeterized approach will become more secure than is currently possible in an open, platform-independent information sharing environment.

6.5. Summary

The three step approach to evaluating the advanced mechanisms for defining, modifying and enforcing data-level access control policy for information shared in distributed, collaborative environments has been tested using the testing strategy. The evidence demonstrates that it is indeed possible to take security labelling to a finer level of granularity and apply it within information resources, which is an implementation of the new granular access control formula. This is an enhancement of what is currently possible within existing access control technology. It is also proven that it is possible to enforce these controls outside the perimeter, through the classification labels being securely embedded within the information as it travels around the distributed Internet, while keeping the access privileges component of the access control policy under the control of the information owner. This is an implementation of the de-perimeterized access control formula and obeys the de-perimeterized linkage rule. This not only allows the access control policy to be applied outside the perimeter of organisational information systems, but it also supports the

modification of access control policy such that any changes are immediately enforced on any network. Something not currently possible in access control technology.

One of the standout dependencies of this approach is a live connection to the Internet. Without that connectivity it is impossible to request access to distributed information. That is not to say that the information becomes any less secure. It remains in its encrypted form until an access request can be made. But in terms of availability, one of the key requirements of Information Security, it can mean the information is unavailable at times. Clearly this is not acceptable with critical information relating to human life or national infrastructure so further work is needed to address this issue. Perhaps time-based tokens could be issued while offline. This has been identified as an issue for further work.

For the purposes of supporting the hypothesis, the implementation and evaluation of the prototype application has provided evidence that the new formulae and rules can be implemented, and that security can be advanced to the point where information sharing can be made much more effective due to increased granularity in classifying and labelling information with security requirements, and enforcing controls in distributed collaborative environments while, importantly, retaining control over the access control policy so that modifications can be made to the policy even after information has been shared beyond the current perimeterized point of control.

For the purposes of providing advancement to current access control models and technology, the mechanisms developed in support of the hypothesis provide an implementation of the industry-recognised De-P security model. The system threat model and risk assessment of existing access control technology, when used to share information in collaborative distributed environments such as VOs, define risks that have been largely mitigated by the functionality available in these new mechanisms. Although there is new risk presented in the de-perimeterized implementation, the existing risks have been greatly reduced and information sharing has the capability to become more inherently secure across organisational boundaries, dynamic in its security controls and permanent in its control of information.

Chapter 7 - Conclusion

The main aim of this research was to define a framework that would provide a platform for the enhancement of existing access control approaches, to allow individuals and businesses to share information required for collaboration where, previously, limitations in technology may have restricted their ability to share such information, due to: small amounts of highly restricted content in a resource raising the classification of the entire resource or; the requirement to retain sustained control over the information to comply with data protection laws. Also, to reduce the likelihood of the kind of information exposures and losses that have been reported recently.

The motivation for the research, based on observations of real-world security breaches and scenarios, indicated that important issues needing to be addressed were:

- Enabling a refined, granular classification and labelling of information so that reflects varying levels of content security requirements within an information resource could be enforced.
- Defining, modifying and enforcing an access control policy on information shared outside the perimeter in distributed collaborative Internet connected environments.

Thus, the hypothesis of the research was:

A document's content can have security enforced at different levels of granularity within the overall document, and the rules defining its access control are always modifiable and enforceable in an Internet connected environment, no matter where the document is held.

In support of these claims, the research has contributed several formulae and rules, detailed in Section 4.3.2, all based on an access control framework that was developed throughout Chapters 3 and 4, and is summarised in Section 4.4.

The basic access control framework developed through this research includes components that are required to model a distributed collaborative computing scenario, and allow formulae to be defined that represent an information resource owner's

boundaries of control in distributed collaborative environments, and the level of granularity to which security should be applied to information resources. The framework is an important reference point from which risks to information can be defined, as limitations of control are clearly identified.

It was determined that two key parts of access control are: decision and enforcement. Figure 7.1 illustrates the fundamental elements of decision-making. The basic access control function $f(c_{ku}, c_{kd}, a_i, r_o)$, is used to evaluate access control requests using a rule-base. The rule base could be an ACL, a rule-based access control or a role-based access control table. The evaluation of access requests can also be informed by an information classification scheme, which is used to determine a user's access control privileges. Fundamentally, if a system exists that has an application that implements the access control decision function, a rule-base, and an information classification scheme, access control decisions can be made, no matter what mode of implementation is chosen or what the classification scheme is, as long as it interacts as shown in Figure 7.1. The research showed that enforcement of access control policy, and not decision making, was the problem in distributed collaborative working. The risks were coming from information being classified as entire resources with respect to security level, and being shared outside the perimeter. It was clear that enforcement controls needed enhancing to deal with these needs.

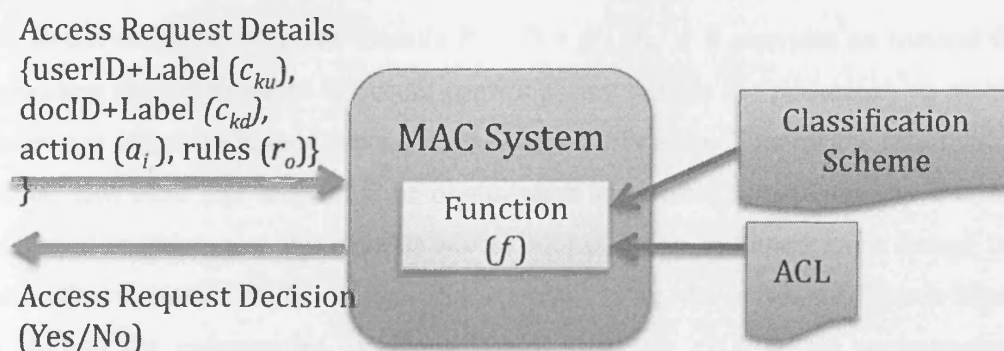


Figure 7.1 – The MAC Approach

With regard to access control enforcement, the granular access control formula $r_a = c_{ku} + \{=, >=, <=, >, <\} + c_{kd}$, where $c_{kd} \in c_k$ provides a basis to allow security to be enforced at different levels of granularity within a document. The requirements for this formula to hold true are that there exists users (u_z), documents (d_x), and an

information classification scheme (c_k) of security labels that can be applied to both users and documents. There must also exist a rule-base that can be used to represent relationships between users and documents, and can be evaluated with a Boolean result that can be used to allow or deny access, as per Figure 7.1. It was determined that most security systems could support this configuration and therefore could support the implementation of the formula. A limitation of the formula is that labels must be applicable within the body of a document to achieve granular access. Chapter 5 detailed an implementation of the formula that worked with XML documents, which was tested in Chapter 6, and demonstrated that it was possible to implement the formula. It is expected that the formula should also hold true for databases, as they are reference-able data structures (columns/rows) that can be searched for labels, and can have upper and lower boundaries (Column X, Rows Y to Z, for example), that hold information in a classifiable container. It is an accepted limitation that the formula may not hold true where the content is not so easily reference-able, such as images and proprietary document formats. The formula works by assigning each user a label from a classification scheme, and the specific sections of a document, such as paragraphs and lines of text, are also assigned labels from the same scheme. Using an access control system that implements the access control function, the user's label can be evaluated against the labels used for document sections. This means access control can be refined to the content with a document as well as the document in its entirety.

The de-perimeterized element formula $P_z = D + \{r_1...r_n\} + E$ provides an method for supporting the enforcement of access control policy outside the perimeter, no matter where it is stored within an Internet connected environment. This means information can be sent from one individual or organisation to another, stored on any Internet connected machine, and still have its access control policy enforced, even though the destination is outside of the owner's locus of control i.e. the perimeter. This is based on shifting the enforcement mechanisms that currently exist within perimeterized environments, outside the perimeter, and making them accessible within all perimeters. By doing this, if information moves outside the perimeter as it often does for collaborative working arrangements, the policy enforcement mechanisms are available and able to enforce the policy. However, this only works if the access control policy either moves to, or is accessible from, the location of the information. In order for access control policy to be enforced on information outside the perimeter,

and for the owner to be able to modify the access control policy for an information resource and see the changes take effect on information previously shared outside the perimeter, the de-perimeterized linkage rule was created. This rule creates a permanent link between the document (d_x), its access control policy (rules) $\{r_1...r_n\}$, the appropriate rule enforcement controls (e_b), and the resource owner themselves (P_z). This must be true for the de-perimeterized formula to be applicable. The rule states there must exist a permanent link between a document d_x , e_b , $\{r_1...r_n\}$, and P_z . This was implemented in the prototype application documented in Chapter 5, and tested in Chapter 6, however, there is a very obvious limitation with this approach, which is if the any of those entities do not have access to the Internet for whatever reason or become unreachable, such as when working on an airplane or remote location, the rule cannot be true. However, the hypothesis stated that the claims were only associated with information stored in an Internet-connected environment, so this limitation and set of situations means the information is not currently held in such an environment.

7.1. Contributions

Thus, the research has made several contributions to the information security and collaborative working domains.

The formulae and rules documented in Chapter 4, and the prototype implementation of these, documented in Chapter 5, demonstrated that different sections in an information resource can be classified based on different security requirements. This is an advance on the traditional method of classifying information resources as a single entity, which results in the withholding of information that would be useful to share with collaborators, because of a small amount of sensitive information within the resource. This enhancement allows small amounts of sensitive information to be classified and restricted from users from outside the organisation, while the rest of the resource can be shared. The impact of this is that a greater amount of information will be able to be shared within collaborative working arrangements. The electronic patient record is a good example of this. A complete patient record contains a great deal of sensitive information, that a patient is obliged to keep private, but also needs to be able to share different parts with different people. For this reason, the entire

resource cannot be shared with all other healthcare professionals. The prototype application allows the sensitive information to be restricted to a patient's GP alone, while other information, such as scans, biopsies and other information can be shared with members of the medical team treating the patient, in such a way that the sharing reflects the role of the user in the treatment.

Additionally, the approach addresses the issue of resource owners not being able to have confidence that their information could be adequately controlled outside their own secured perimeter. This is due to the approach having the ability to maintain control over the access control policy for the information, even after it has been shared. Changes to the UK Data Protection Act (1998) mean there are stricter controls and harsher penalties for data controllers of personally identifiable information who do not enforce these controls. This affects any individual or organisation that shares information with other parties, in collaborative working environments, whether in academic, industry or healthcare domains. This situation has the potential to cause a lock-down of data to avoid such penalties due to the increased accountability of the data owner. This is a limiting factor on the potential for collaboration. In fact, in the light of the loss of 25 million personal records, Her Majesty's Revenue and Customs (HMRC), did just that on the advice of the Government. The identified de-perimeterized access control formula and linkage rule provides a framework, which supports access control policy enforcement of information outside the perimeter. Consider the HMRC data losses. Information was stored on discs and sent to a recipient at the Office of National Statistics (ONS). The discs were lost, and the whereabouts of the data was unknown. If de-perimeterized access control had been used, as described in Chapter 5, to classify the personal data on those discs, the data loss could have had much less impact, as only an authenticated user would have been able to read what was on the discs. Thus, even though the discs were lost, the data on them would have been unreadable by anyone who found them, unless they had the required access rights.

Furthermore, the de-perimeterization developments allow an access control policy to not only be enforced remotely, but to be retained and modified from a central point by the information resource owner. This has many implications. Given the HMRC data loss, the HMRC could have revoked all access previously granted to the lost data,

meaning nobody in the future, not even an authenticated employee who received the lost package a few weeks later, would be able to access the data. This achieves complete information redaction after it has been shared. Something that was not previously possible. In the healthcare collaboration, once a patient's care is complete, access to the parts of a patient record shared with other organisations treating the patient can be revoked. This removes any further access to patient information. The Data Protection Act (1998), requires "appropriate protection" to be given to personal information. There is a strong argument for the requirement to share patient information. The more information healthcare professionals have about the patient, the better informed they are when making treatment choices. However, they only need this access while they are treating the patient. It is no longer appropriate for them to have access to the information after the care is complete. Previously, there was no way of revoking access to this information. Therefore, the de-perimeterization and granular access control approaches can enable more "appropriate protection", because it allows legitimate access to personal information to be revoked after the requirement for its access is no longer present.

7.2. Future Work

The prototype application demonstrates the capability to implement the new formulae and achieve de-perimeterized access control for XML content, which can be extended to proprietary content by converting it to XML through open-source Web Services. Applying labels to a structured resource means that the approach could feasibly be used for more than standard text documents. Databases are also structured resources. Much of the online content produced in Web pages, wikis, blogs and social networking content, is actually derived from a database back end. If the fields of a database could be classified using labels, the approach could feasibly be used to enforce access control for information displayed online. When a query extracts data from a database, the labels that classify the various fields that produce the results of the query could be inspected and, depending on the identity of the user making the request for access, restricted accordingly. Indeed, referring again to the HMRC data loss, the information that was stored on the lost discs was generated from a large dataset resulting from a database query. If the database had "built-in" labels that

classified the personal data as restricted outside the organisation, it could have been automatically encrypted and restricted to named recipients, using this approach.

Building on the idea of automated content restriction from database queries, another use for the approach could be in the automatic restriction of information flow outside an organisation. People often share information through attachments to email messages, or in the email message itself. There are tools available to scan the content of outgoing messages and flag up instances of specific terms and content to the user, prompting them to consider the security of the message they are sending. If, when prompted, they were given a set of security labels to choose from, an implementation of the approach could be used to automatically classify the flagged content, encrypt the content, and require user authentication and access control through the de-perimeterized client, before allowing access to it. This has wider implications in terms of management and usability. The time involved in implementing this level of security, and its ease of use by users, would require investigation as to whether it involved unacceptable overheads. However, the semantic analysis of information resources, whether they are emails, documents or databases, is an interesting concept for future investigation.

It is questionable whether complete security can ever be made possible, given that the “Analog hole” problem means information can always be reproduced after a person has read it. Even with system level controls to prevent printing, copying or screen dumping, the reader can always reproduce the information from memory or by working around system level controls by photographing the screen and re-typing information. As the de-perimeterized access control formula and linkage rule enable a permanent link between an information resource and its owner, requiring communication between user and resource owner on every request for access, it could be used to create an auditable log of access requests in support of Clark-Wilson’s well-formed transaction. This has the potential to allow investigation of the legal stance in future. Audit information could be used to present a case for prosecution in an alleged misuse case. The requirements for court admissibility of this type of information are a grey area. There is a recent standard published that defines the legal admissibility of electronic evidence [BS08], which would need further investigation, but the de-perimeterized logic provides a foundation to build on the collection of

information required to create such cases. Auditable access request logs could provide back-up for collaboration agreements, where shared information is to be returned at the end of collaboration. The system already provides a sustained link between the information resource and its owner. If there was any evidence of collaborators using the information after the end of a collaboration, the capability to extract an access control policy history from the logs that, together with the collaboration agreement, prove the person had agreed not to further use the information and that access had been revoked, would allow the creation of a misuse case against the collaborator if they violate the agreement.

To conclude, the research in this thesis has made significant advances in information security methods and technology, particularly with respect to information shared in collaborative working environments. The ability to drill down into a resource and control access to different sections of its content depending on their security requirements will allow more information to be shared, where previously large parts of information resources were restricted due to a small amount of sensitive information. The ability to share information while retaining control of its access control policy and having modifications to the policy enforced on information outside an organisation's perimeter, gives the resource owners a control that they do not currently have. De-perimeterization is a recognised ideology, but there is very limited published research on its implementation. This thesis contributes to that domain. The section on future work highlights there is plenty of directions this research could take in the future. The evaluation also shows that there are still some issues to be addressed to improve the implementation of the formulae and rules. The results however, prove that a significant advance has been made to access control for information shared in distributed collaborative environments.

References

- [AALY06] Abelson, H. Adida, B. Linksvayer, M. & Yergler, N. ccREL: The Creative Commons rights Expression Language. March 2006. Retrieved August 28, 2009 from <http://wiki.creativecommons.org/images/d/d6/CcREL-1.0.pdf>
- [ACC+03] Alfieri, A. Cecchini, R. Ciaschini, V. Frohner, A. Gianoli, A. Lorentey, K. & Spataro, F. VOMS: an Authorization System for Virtual Organizations. Proceedings of the *1st European Across Grids Conference*, Santiago de Compostela, 2003.
- [AKE] Akenti Project Website. Retrieved August 28, 2009 from <http://acs.lbl.gov/Akenti/>
- [And08] Anderson, R. *Security Engineering*. Wiley, 2008.
- [BCF+04] Bertino, E. Carminati, B. Ferrari, E. Thuraisingham, B. & Gupta, A. Selective and Authentic Third-Party Distribution of XML Documents. *IEEE Trans. on Knowl. and Data Eng.* 16, 10 (Oct. 2004), 1263-1278.
- [Bel05] Bell, D. Looking Back at the Bell-La Padula Model. Proceedings of the *21th Annual Computer Security Applications Conference*, Tucson, Arizona, December 5-9, 2005
- [BERR08] BERR Information Security Breaches Survey 2008. April 2008. Retrieved August 28, 2009 from http://www.pwc.co.uk/eng/publications/berr_information_security_breaches_survey_2008.html
- [BFPW07] Boldyreva, A. Fischlin, M. Palacio, A. & Warinschi, B. A Closer Look at PKI: Security and Efficiency. *Public Key Cryptography*, Vol. 4450 Springer (2007), p. 458-475.
- [BHL01] Berners-Lee, T. Hendler, J. & Lassila, O. The Semantic Web. *Scientific American*. May 17, 2001. Retrieved August 28, 2009 from http://www.si.umich.edu/~rfrost/courses/si110/readings/in_out_and_beyond/semantic_web.pdf

- [Bib77] Biba, K. J. Integrity Considerations for Secure Computer Systems. Technical Report. ESD-TR-76-372, USAF Electronic Systems Division, Bedford, MA, Apr. 1977, (Also available through National Technical Information Service, Springfield Va., NTIS AD-A039324.).
- [BPJ+05] Burnap, P. Pahwa, JS. Joita, L. Gray, A. Rana, O. & Miles, J. Grid Based E-Procurement. Proceedings of *the 2005 International Conference on Computing in Civil Engineering*, Cancun, Mexico, 12-15 July 2005, published on CD by ASCE Reston Virginia USA, ISBN 1-703-295-6163.
- [BN89] Brewer, D & Nash, M. The Chinese Wall Policy. Proceedings of the *IEEE Symposium on Research in Security and Privacy*, Oakland, California, May 1989.
- [BOE] Boeing 787 Dreamliner Technical Specifications. Retrieved August 28 2009 from <http://www.boeing.com/commercial/787family/programfacts.html>
- [Brag06] Bragg, R. *Certified Information Systems Security Professional*. Que, 2003.
- [BS08] BS 1008:2008 Evidential weight and legal admissibility of electronic information. Specification. Retrieved August 28, 2009 from <http://www.bsi-global.com/Shop/Publication-Detail/?pid=000000000030172973>
- [CAGL97] Camarinha-Matos, L.M. Afsarmanesh, H. Garita, C. & Lima, C. Towards an Architecture for Virtual Enterprises. Proceedings of the *2nd World Congress on Intelligent Manufacturing Processes & Systems*, Budapest, June 1997.
- [Cas00] Cascio, W. Managing a Virtual Workplace. *The Academy of Management Executive (1993)*, Vol. 14, No. 3, Themes: Structure and Decision Making (Aug., 2000), pp. 81-90.
- [CCMW01] Christensen, E. Curbera, F. Meredith, G. & Weerawarana, S. Web Services Description Language (WSDL) v1.1. W3C Note. 15 March 2001. Retrieved August 28, 2009 from <http://www.w3.org/TR/wsdl>

- [CHY+98] Chung, P. Huang, Y. Yajnik, S. Liang, D. Shih, J. Wang, C.-Y. & Wang, Y. DCOM and CORBA side by side, step by step, and layer by layer. *C++ Report*, Vol. 10, No. 1, pp. 18-29, 40, Jan. 1998 .
- [CLO97] Camarinha-Matos, L.M. Lima, CP, & Osorio, L. The PRODNET platform for production planning and management in virtual enterprises. Proceedings of *ICE'97- Int. Conf. On Concurrent Enterprising*, Nottingham, UK, Oct 97.
- [CO02] Chadwick, D.W. & Otenko, A. The PERMIS X.509 Role Based Privilege Management Infrastructure. Proceedings of the *7th ACM Symposium on Access Control Models and Technologies*, 2002.
- [CW87] Clark, D. Wilson, D. A Comparison of Commercial and Military Computer Security Policies. Proceedings of the *IEEE Symposium on Security and Privacy*, 1987.
- [DCPS02] Damiani, E. De Capitani di Vimercati, S. Paraboschi, S. & Samarati, P. A fine-grained access control system for XML documents. *ACM Trans. Inf. Syst. Secur.* 5, 2 (May. 2002), 169-202.
- [Den97] Denning, D. A lattice model of secure information flow. *Communications of the ACM* 19, 5: 236–243
- [DOD85] US Department of Defense, *Department of Defense. Trusted Computer System Evaluation Criteria. DoD 5200.28-STD*, Washington, D.C., US Department of Defense, Dec. 1985.
- [DPA98] The UK Data Protection Act (1998). Retrieved August 28, 2009 from http://www.opsi.gov.uk/Acts/Acts1998/ukpga_19980029_en_1
- [DV] DocVert Website. Retrieved August 28, 2009 from <http://holloway.co.nz/docvert/>
- [ECMA08] Standard ECMA-376. Office Open XML File Formats 2nd edition. (December 2008). Retrieved August 28, 2009 from <http://www.ecma-international.org/publications/standards/Ecma-376.htm>
- [FK92] Ferraiolo, D.F. & Kuhn, D.R. Role Based Access Control. Proceedings of *15th National Computer Security Conference*, October 1992. 554-563.

- [FKT01] Foster, I. Kesselman, C. & Tuecke, S. The Anatomy of the Grid: Enabling Scalable Virtual Organizations. *Supercomputer Applications*, 15(3), 2001.
- [FKNT02] Foster, I. Kesselman, C. Nick, J. & Tuecke, S. The Physiology of the Grid: An Open Grid Services Architecture for Distributed Systems Integration. Proceedings of the Open Grid Service Infrastructure WG, *Global Grid Forum*, June 22, 2002.
- [God03] Godwin-Jones, R. Blogs and Wikis: Environments for On-line Collaboration. *Language Learning & Technology*. May 2003, 7(2): 12-16.
- [Hay08] Hayes, B. Cloud computing. *Commun. ACM*, 51, 7 (Jul. 2008), 9-11.
- [HBT07] Hilton, J. Burnap, P & Tawileh, A. Methods for the identification of Emerging and Future Risks. Report Commissioned by the European Network and Information Security Agency (ENISA), 2007. Retrieved August 28, 2009 from http://www.enisa.europa.eu/doc/pdf/deliverables/EFR_Methods_Identification_200804.pdf
- [Hom05] Hommel, W. Using XACML for privacy control in SAML-based identity federations. *Lecture notes in Computer Science*. 2005, 3677, pages 160-169 ISSN 0302-9743
- [ISO96] ISO/IEC 10181-3:1996. Retrieved August 28, 2009 from http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=18199
- [ISO05] ISO/IEC 27001:2005. Information technology -- Security techniques - Information security management systems – Requirements. Retrieved August 28, 2009 from http://www.iso.org/iso/catalogue_detail?csnumber=42103
- [Jer07] Jericho Forum Whitepaper. Business rationale for de-perimeterisation. Retrieved August 28, 2009 from http://www.opengroup.org/jericho/Business_Case_for_DP_v1.0.pdf
- [Jer09a] Jericho Forum Position Paper. Information Lifecycle Management. Retrieved August 28, 2009 from

http://www.opengroup.org/jericho/COA_Information_Lifecycle_Management_v1.0.pdf

[Jer09b] Jericho Forum Position Paper. Collaboration Oriented Architectures. Retrieved August 28, 2009 from http://www.opengroup.org/jericho/COA_v2.0.pdf

[JF09] Jericho Forum Position Paper. Information Classification. Retrieved August 28, 2009 from http://www.opengroup.org/jericho/COA_InformationClassification_v1.0.pdf

[KFJG06] Kagal, L. Finin, T. Joshi, A. & Greenspan, S. Security and Privacy Challenges in Open and Dynamic Environments. *Computer* 39, 6 (Jun. 2006), 89-91.

[KSR07] Krishnan, R. Sandhu, R. & Ranganathan, K. PEI models towards scalable, usable and high-assurance information sharing. Proceedings of the *12th ACM Symposium on Access Control Models and Technologies*, Sophia Antipolis, France, June 20 - 22, 2007.

[LHM84] Landwehr, C. E. Heitmeyer, C. L. & McLean, J. A security model for military message systems. *ACM Trans. Comput. Syst.* 2, 3 (Aug. 1984), 198-222.

[Lin05] Lindner, R. SWAMI - Safeguards in a World of Ambient Intelligence. Report. 2005. Retrieved August 28, 2009 from <http://www.securitytaskforce.org/dmdocuments/SWAMI.pdf>

[LSS03] Liu, Q. Safavi-Naini, R. & Sheppard, N. P. Digital rights management for content distribution. Proceedings of the *Australasian Information Security Workshop Conference on ACSW Frontiers*. Adelaide, Australia, 2003.

[LZWQ05] Li, H. Zhang, X. Wu, H. & Qu, Y. Design and Application of Rule Based Access Control Policies. Proceedings of the *Semantic Web and Policy Workshop*, held in conjunction with the *4th International Semantic Web Conference*, 7 November, 2005, Galway Ireland. 34-41

[Mis03] P. Mishra et al. Differences between OASIS Security Assertion Markup Language (SAML) V1.1 and V1.0. OASIS Draft, May 2003. Retrieved August 28, 2009 from <http://www.oasis-open.org/committees/download.php/3412/sstc-saml-diff-1.1-draft-01.pdf>

- [Mit05] Mitchell, C. Trusted Computing. *IEEE Professional Application of Computing*. Series 6. Retrieved August 28, 2009 from <http://books.google.co.uk/books?id=9iriBw2AuToC&printsec=copyright&dq=trusted+computing&lr=#PPP1,M1>
- [Mur07] Murphy K. Gates Plugs Obvious Borderless Security Vision. Article in *Computer Business Review Online* – 7th February 2007. Retrieved August 28, 2009 from http://www.cbronline.com/article_news_print.asp?guid=CE19F4C0-28BA-4BF2-A746-8ABA4985DB18
- [MSFAQ] Microsoft Next-Generation Secure Computing Base - Technical FAQ. Retrieved August 28, 2009 from <http://technet.microsoft.com/en-us/library/cc723472.aspx>
- [NHS] NHS National Encryption Framework. Specification. Retrieved August 28, 2009 from <http://www.wales.nhs.uk/ihc/page.cfm?pid=34112&orgid=770>
- [NSRA07] Newhouse, S. Schopf, J. Richards, A. & Atkinson, M. Study of User Priorities for e-Infrastructure for e-Research (SUPER). Proceedings of *the UK e-Science All Hands Meeting*, September 2007.
- [One03] O'Neill et. Al. *Web Services Security*. Osborne, 2003. ISBN 0-07-222471-1
- [Ore07] Oreilly, T. What is Web 2.0: Design Patterns and Business Models for the Next Generation of Software. *Communications & Strategies*, No. 1, p. 17, First Quarter 2007.
- [Pal05] Palmer, G. De-Perimeterisation: Benefits and limitations. *Information Security Technical Report*, 2005. Vol. 10. Num 4. ISSN: 1363-4127.
- [PCC+06] Periorellis, P et. Al. Service Oriented Middleware for the Formation and Operation of Virtual Organisations: The GOLD Project. University of Newcastle upon Tyne: Computing Science. 2006. Technical Report Series No. CS-TR-940.
- [PCH+06] Periorellis, P. Cook, N. Hiden, H. Conlin, A. Hamilton, M.D. Wu, J. Bryans, J. Gong, X. Zhu, F. & Wright, A. GOLD Infrastructure for Virtual

Organisations. Proceeding of the *UK e-Science All Hands Meeting 2006*, Nottingham, UK.

[PL03] Perrey, R. & Lycett, M. Service-Oriented Architecture. Proceedings of the *SAINT Workshops 2003*: 116-119

[PR04] Park, J. & Ram, S. Information systems interoperability: What lies beneath?. *ACM Trans. Inf. Syst.* 22, 4 (Oct. 2004), 595-632.

[PWF+02] Pearlman, L. Welch, V. Foster, I. Kesselman, C. & Tuecke, S. A Community Authorization Service for Group Collaboration. Proceedings of *Policies for Distributed Systems and Networks International Workshop*, POLICY 2002.

[SCD+08] Sinnott, R. Chadwick, D. Doherty, T. Martin, D. Stell, A. Stewart, G. Su, L. & Watt, J. Advanced Security for Virtual Organizations: The Pros and Cons of Centralized vs Decentralized Security Models," Proceedings of the *Eighth IEEE International Symposium on Cluster Computing and the Grid (CCGrid)*, 2008.

[SCFY96] Sandhu, R. Coyne, E.J. Feinstein, H.L. & Youman, C.E. Role-Based Access Control Models. *IEEE Computer* 29 (2): 38–47. (August 1996).

[SCK+06] Sinnott, R. Chadwick, D. Koetsier, J. Otenko, O. Watt, J. & Nguyen, T.A. Supporting decentralized, security focused dynamic virtual organizations across the grid. Proceedings of the *Second IEEE International Conference on e-Science and Grid Computing 2006 (e-Science '06)*, December 2006, pages pp. 22-22, Amsterdam, The Netherlands.

[She00] Shen, W. Virtual Organizations in Collaborative Design and Manufacturing Systems, *Journal of Organizational Virtualness*, 2(2), 43-58, 2000.

[Shib] Internet2 Shibboleth Technology Website. Retrieved August 28, 2009 from <http://shibboleth.internet2.edu>

[Sie08] Lee Siegel. *Against the Machine. Being Human in the Age of the Electronic Mob*. Serpent's Tail, 2008.

[SS94] Sandhu, R. & Samarati, P. Access control: Principles and practice. *IEEE Communications* 32, 9, 40-48. 1994.

- [Sta02] Stamp, M. Digital Rights Management: The Technology Behind the Hype. *Journal of Electronic Commerce Research*; 2003, Vol. 4 Issue 3, p102-112.
- [SZRC06] Sandhu, R. Zhang, X. Ranganathan, K. & Covington, M. Client-side access control enforcement using trusted computing and PEI models. *J. High Speed Networks* 15(3): 229-245 (2006).
- [TJM+99] Thompson, M. Johnston, W. Mudumbai, S. Hoo, G. Jackson, K. & Essiari, A. Certificate-based Access Control for Widely Distributed Resources. Proceedings of the *8th Conference on USENIX Security Symposium - Volume 8* (Washington, D.C., August 23 - 26, 1999). USENIX Security Symposium.
- [TW08] Thomas, R & Walport, M. Data Sharing Review. Report. July 2008. Retrieved August 28, 2009 from <http://www.justice.gov.uk/reviews/docs/data-sharing-review-report.pdf>
- [Var02] Vartiainen, M. The functionality of virtual organizations. Proceedings of the *International Conference of T-World* 2001, Helsinki.
- [VC02] Velez, F.J. & Correia, L.M. Mobile broadband services: classification, characterization, and deployment scenarios. *Communications Magazine, IEEE*. Volume 40, Issue 4, Apr 2002 Page(s):142 – 150
- [Vin97] Vinoski, S. CORBA: integrating diverse applications within distributed heterogeneous environments. *Communications Magazine, IEEE*. 35, 2, 46-55. ISSN: 0163-6804
- [VPM] VPM Project Website. Retrieved August 28, 2009 from <http://sec.cs.kent.ac.uk/vpman/>
- [W3C99] XML Path Language (XPath) Version 1.0. Specification. W3C Recommendation. Retrieved August 28, 2009 from http://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/techops/atc_comms_services/swim/documentation/media/compliance/Xpathv1.0.pdf
- [WKSS06] Watt, J. Koetsier, J, Sinnott, R. Stell, A. DyVOSE Project: Experiences in Applying Privilege Management Infrastructures. Proceedings of *UK All Hands*

Meeting, 18-21st September 2006, East Midlands Conference Centre, Nottingham, England.

[WSF+03] Welch, V. Siebenlist, F. Foster, I. Bresnahan, J. Czajkowski, K. Gawor, J. Kesselman, C. Meder, S. Pearlman, L. & Tuecke, S. Security for Grid services. Proceedings of *12th IEEE International Symposium on High Performance Distributed Computing*, 2003.

[WSJ07] Watt, J. Sinnott, R. & Jiang, J. GLASS Project: Supporting Secure Shibboleth-based Single Sign-On to Campus Resources. Proceedings of *UK All Hands Conference*, 2007.