

UNIVERSITY OF OSLO
Department of Informatics

**Evaluation of file
access control
implementations**

Master thesis

Fatima A. Mader

May 2005



Acknowledgement

I would like to thank my supervisor professor Mark Burgess and Oslo University College for giving me opportunity to write my Master Thesis in Access control Models. I want to thank him for the advice he gave me. I also would like to thank my brother Ahmed A. Madar who supported me a lot in this project.

Oslo, May 2005

Fatima A. Madar

Abstract

This thesis discusses two implementations of file access controls: the *UNIX Permissions* (UP) and the *Access Control List* (ACL).

We will evaluate advantages and weaknesses in these two implementations. The criteria of evaluation are *usefulness*, *security* and *manageability*. The level of usefulness of systems was measured by evaluating user-surveys. The level of security was measured by comparing the implementations against well-established file access control models concerning privacy, integrity, authentication and trust. Manageability was measured by comparing the implementations against a manageability model developed from the field of Human-Computer-interactions.

Preface

This project is a Master Thesis completed at Oslo University College, department of Computer Science in spring 2005.

Contents

Acknowledgement.....	ii
Abstract.....	iv
Preface.....	vi
Contents.....	viii
Abbreviations.....	1
List of Symbols.....	2
Chapter 1.....	4
Introduction.....	4
1.1 Purpose of Project.....	4
Chapter 2.....	6
Background.....	6
2.1 What is File Access Control?.....	6
2.2 Aspects of File Access Control.....	7
2.2.1 Privacy Aspect.....	7
2.2.2 Integrity Aspect.....	8
2.2.3 Authentication Aspect.....	9
2.2.4 Trust Aspect.....	10
2.2.5 Manageability Aspect.....	11
2.3 Security Models.....	12
2.3.1 Bell-LaPadula confidentiality/privacy model.....	12
2.3.2 Biba integrity model.....	13
2.3.3 Clark-Wilson hybrid authentication model.....	13
2.4 What is Human Computer Interaction.....	14
2.4.1 Human-centered designs.....	14
2.5 The main Human-centered HCI Objectives.....	15
2.5.1. Enhancement of human abilities.....	15
2.5.2. Overcome human limitations.....	15
2.5.3. Induce human acceptance.....	15
2.6 HCI in File Access Control.....	16
Chapter 3.....	18
Existing File Access Control Implementations.....	18
3.1 UNIX Permissions (UP).....	18
3.2 Windows Access Control Lists (ACL).....	20
3.3 Comparison: WACL vs. UP FAC logic.....	22
3.4 Comparison: WACL vs. UP User Interfaces.....	24
3.4.1 UNIX User Interfaces.....	24
3.4.2 Windows User Interfaces:.....	25
Chapter 4.....	26
Methodology.....	26
4.1 Research planning.....	26
4.2 Research questions.....	26
4.3 Research Material.....	27

4.4 Questionnaires	27
4.5 Control of data and statistics	28
4.5.1 Tools to control data and statistics	28
4.5.2 Ethical issues	28
4.6 Procedures	28
4.7 Research subjects	29
Chapter 5	32
Results and Analysis	32
5.1 Definitions and Hypotheses	32
5.2 Strategy matrix	34
5.3 Analysis of results from study I and II	34
5.3.1. Description of variables	34
5.3.2 Group 1: Preference	35
5.3.3 Group 2: Usefulness	36
5.3.4 Group 3: Knowledge	37
5.3.5 Group 4: File right management knowledge	38
5.3.6 Group 5: Security	40
5.4. Factors affecting the preference of operative systems	42
Chapter 6	44
Discussion	44
6.1 What makes file access system good ?	44
6.1.2 Security weaknesses	44
6.1.3 Technical quality	45
6.1.4 Method	45
6.1.5 Test participants	46
6.1.6 Participant knowledge	46
6.1.7 Questionnaires	46
6.1.8 Results	47
6.1.9 What could be done differently?	48
6.2 Discussion Summary	49
Chapter 7	50
Conclusion and Recommendations	50
Appendix A	52
Result of Study I	52
Appendix B	54
Questionnaire from Study I	54
Appendix C	60
Results from study II	60
Appendix D	62
Questionnaire from Study II	62
Appendix E	64
Questionnaire from Study II	64
Appendix F	65
Glossary	65
Appendix G	66
Progress Schedule	66

Abbreviations

Multics:	Multiplexed Information and Computing Service
F.A.S:	File Access System
UP:	Unix Permissions
ACL:	Access Control Lists
Entity:	Subject (program , person)
QoS:	Quality of Systems(Ideal system look in Formula1)
FACS :	File Access Control Systems
DFS :	Distributed File System
IP:	Internet address
OUCDE:	Oslo University College Department of Engineering
HCI:	Human Compute Interaction

List of Symbols



: Data/Information



: No allowed to Access Data/file



: Allowed to Access Data /file



:direction arrow

Chapter 1

Introduction

As with all valuables, data need to be protected. The higher the value, the greater is the need for protection. File access systems – a scheme to protect your data from unwanted access - is therefore essential. Unfortunately, not all file access systems are user-friendly. The two most common file access systems in use today are ACL's and Unix-permissions. File System ACLs is difficult to use, but is a powerful tool compare to UNIX permissions, which is simple and primitive. Different users, situations and needs makes for different view of which system is most suitable and efficient.

1.1 Purpose of Project

The purpose of this paper is to compare the UNIX permissions and Windows ACL to evaluate the *Quality of System* of these two systems as they are used by users.

Quality of System is here defined as the total degree of statistical, user-experienced success for a user applying either permission systems for a specific purpose.

The comparison will be based on an evluation matrix assembled from a a selected number of File Access Control models and models for Human Computer Interactions.

Even though there has been several dissertations about the technical aspects of access control implementations, there is little research on the value of any particular implementation from the view of point of the user. The findings from this project will, amongst other things suggest why users rarely use ACL.

Chapter 2

Background

2.1 What is File Access Control?

Security is a very important part of our society today. It is about protecting our property and privacy. We have the situation where there is an amount of information resource that we need to protect to a certain degree from unwanted outsiders, while still letting it is available to certain entities for some specific purpose. File Access Control allows us to secure data stored in computers, more specifically files and folders assigned to users [1].

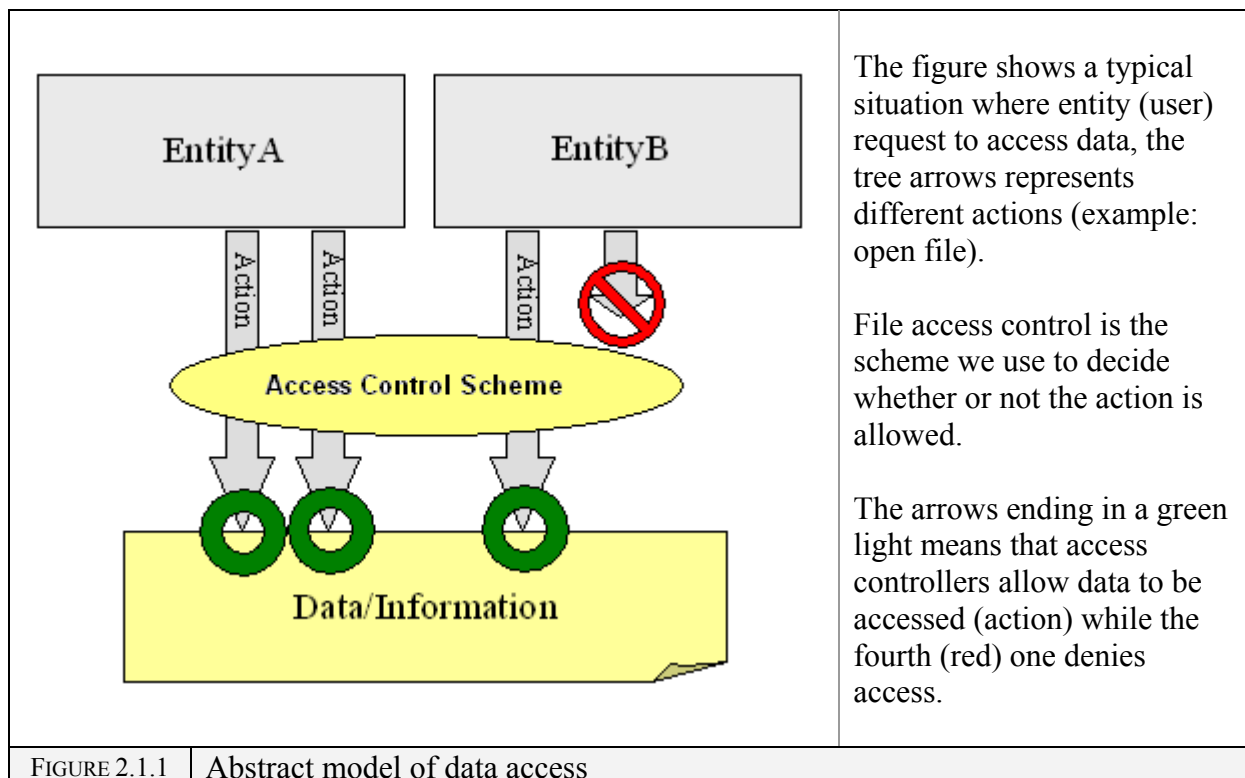


FIGURE 2.1.1 Abstract model of data access

2.2 Aspects of File Access Control

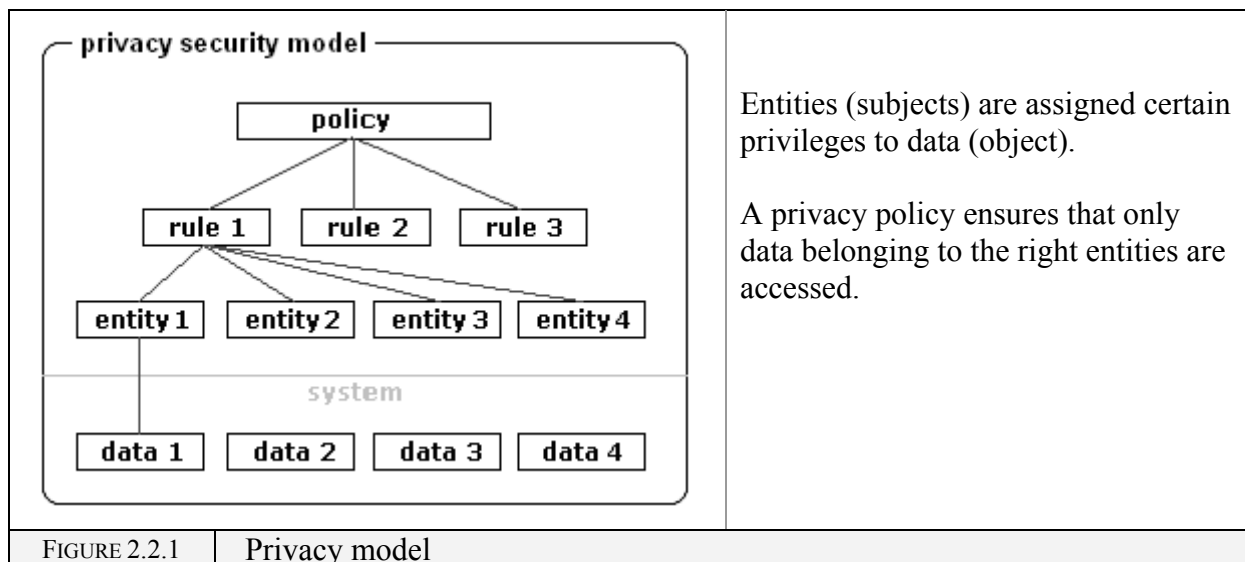
What we commonly associate with file access control is a scheme to protect data from unwanted perusal or editing. This is only a simplification, since files need protections not only from persons but also from programs. More generally therefore, file access control should be defined as 'protecting files from ending up in unwanted states'. There are many aspects to file access control and different levels of protection.

Models for security deal with *five* main aspects of security, namely *privacy*, *integrity*, *authentication*, *trust* and *manageability*. Some models focus on one single aspect, others are hybrids such as the Clark-Wilson model (see 4).

Each model describes a policy that is constituted by a set of rules. All rules must comply to the governing *policy* of the model.

2.2.1 Privacy Aspect

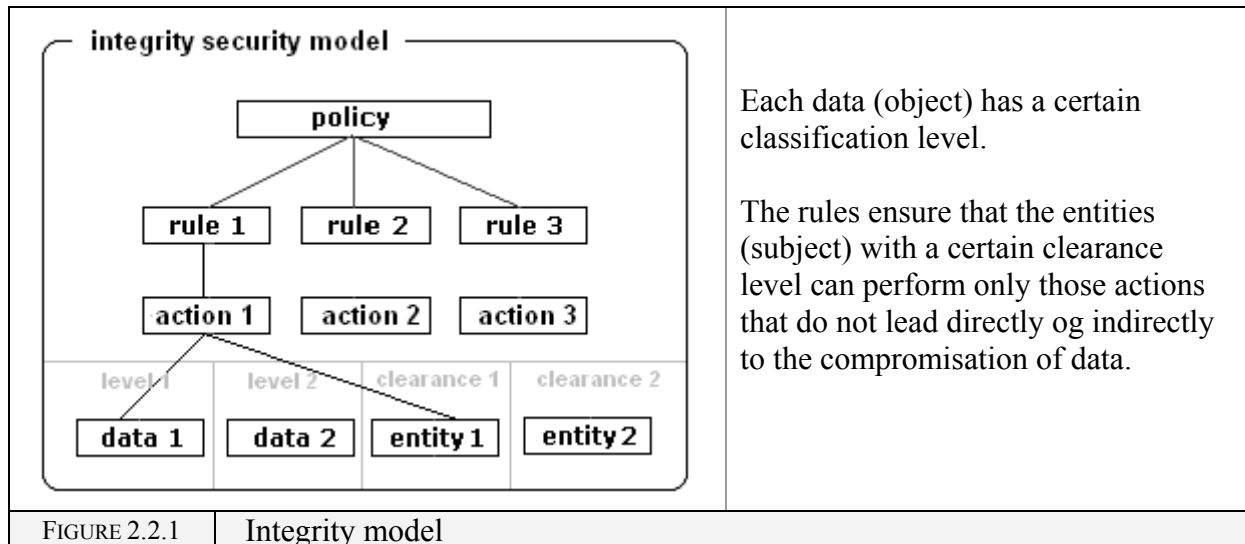
Privacy is the concept where subjects wish to restrict access to objects. A privacy model is about ownership of files. Examples of data that need privacy are exam questions, bank details, and personal data such as medical information.



A *privacy security model* is the collection of *rules* determining who gets access to your data and who doesn't. The most well known model describing privacy is the Bell LaPadula model (see 2.3.1).

2.2.2 Integrity Aspect

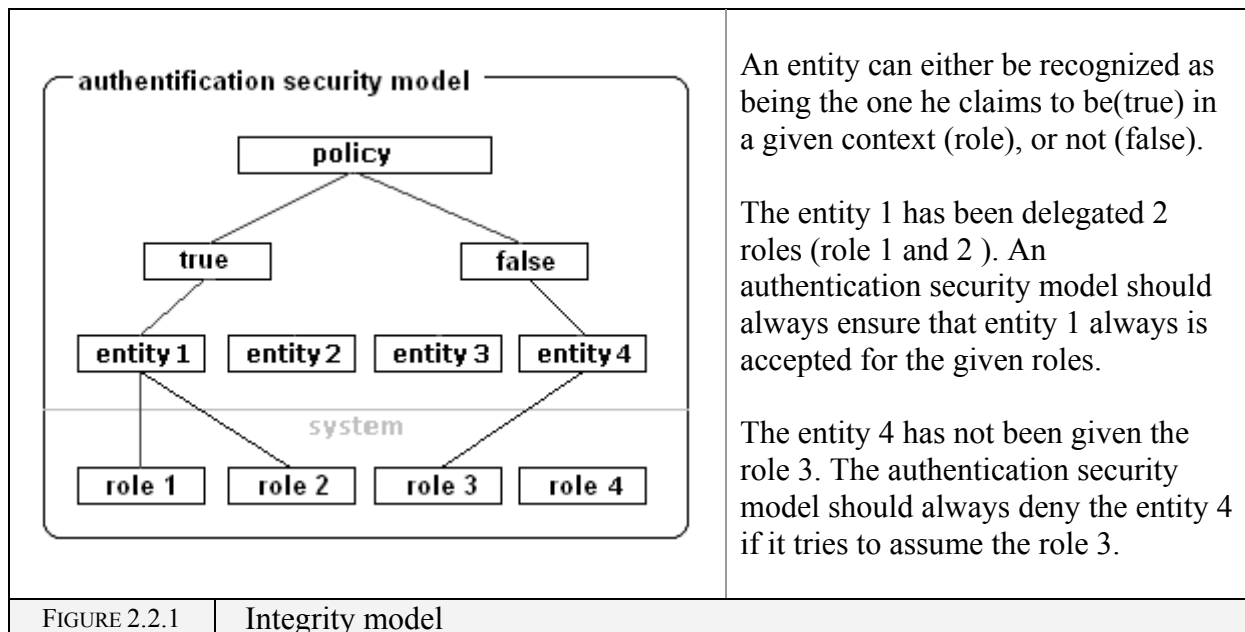
Integrity is based on the concept that data, which can be classified into different levels of purity, can interact with each other and possibly contaminate each other. The concept of purity implies that data exists different states of desirability. Examples of undesired data that corrupts desirable data are viruses spreading through files.



An *integrity security model* is the collection of rules determining which actions are allowed on the data in order to keep them clean. The most well known models describing integrity are the Biba model (see 2.3.2).

2.2.3 Authentication Aspect

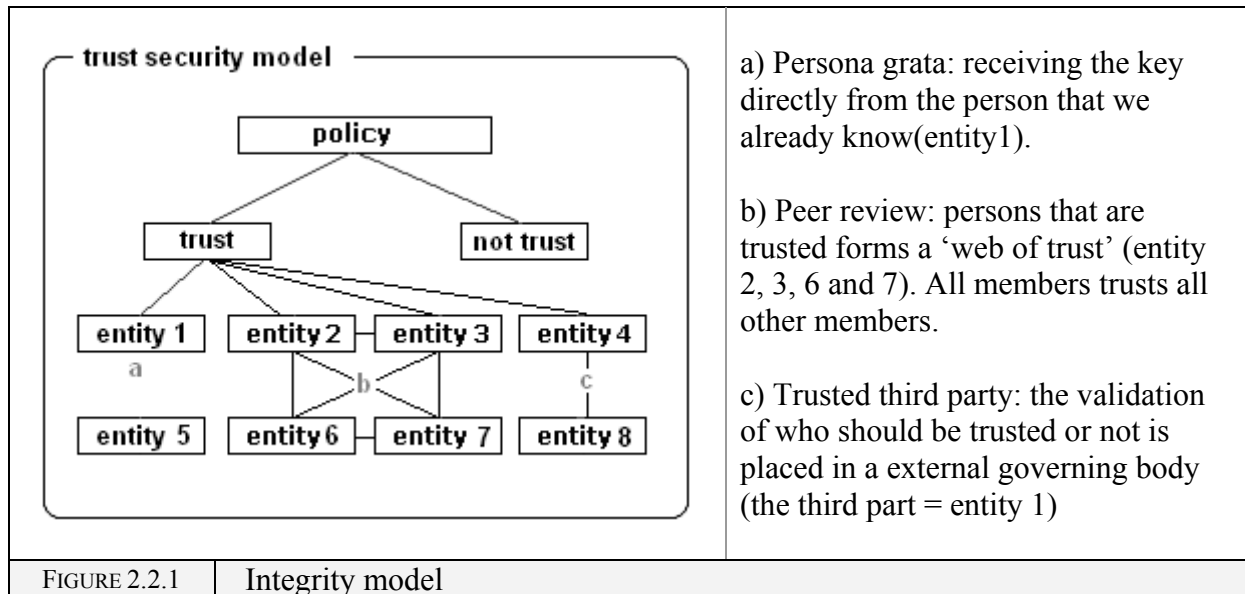
Authentication is how to know someone is really the one he/she claims to be. Examples are net- banks login system where a person has to enter the identification number (social security number) and security code [2].



A *authentic security model* identifies an entity in connection with a certain role. Symmetric and asymmetric schemes are the most common models.

2.2.4 Trust Aspect

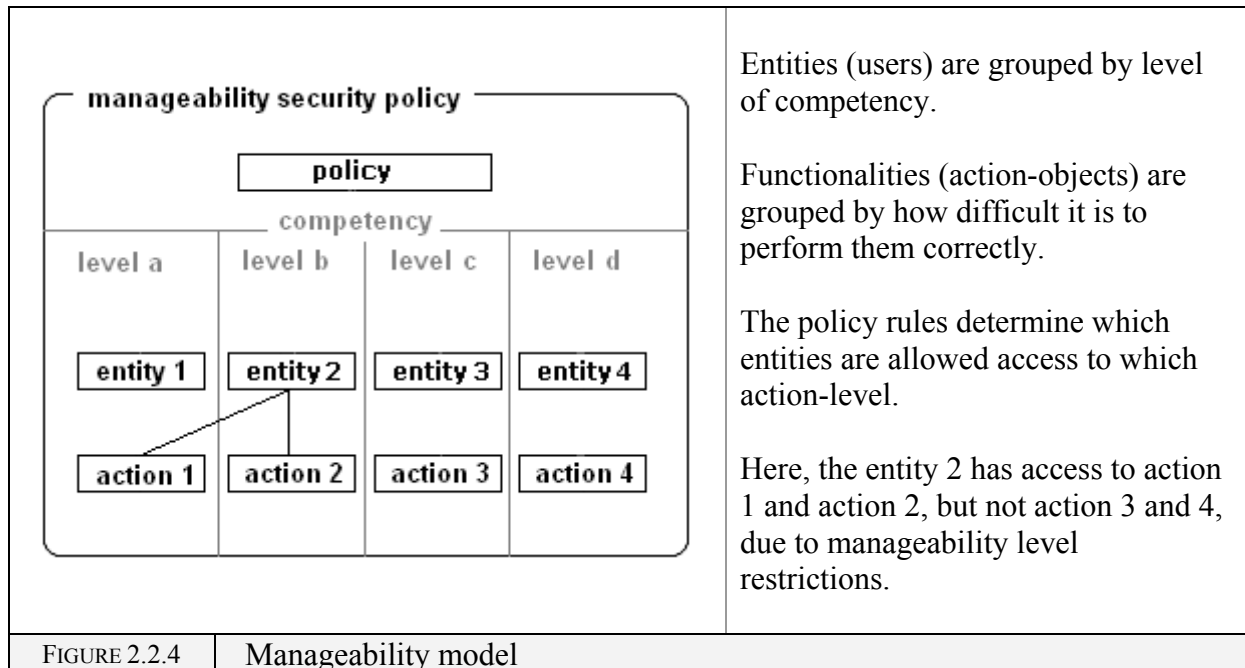
Trust policy describes how the chain of trust should be. An example of a trust issue is the question of who we should trust to give us the keys needed to establish authentication connection.



A *trust security model* describes how trust is interlinked. The most well known models governing authentication is the person grata, the peer review and the third party model (Kerberos model).

2.2.5 Manageability Aspect

A manageability security policy states the rules governing how entities should be exposed to privileged actions. An example of a manageability issue is the question of what the default configuration of a system should be, or how objects are difficult or hazardous, such as system files, are 'hidden' from sight [96,97,98].



A *manageability security model* describes the relation between user knowledge and access rights. This model is general since it does not state specifically what level of action-object an entity of a certain level should be allowed access. It is usually desirable to let users have access to functionalities of same and lower (easier) levels. A typical model handling this aspect is the Role-based access control model[6].

2.3 Security Models

In general, security models provide guidelines to what policies should be in order for a system to be secure, but the actual implementations usually cannot follow the model exactly, and compromises are often made. Following is a selection of the most important models for privacy, integrity, authentication, trust, manageability.

2.3.1 Bell-LaPadula confidentiality/privacy model

The Bell-LaPadula (BLP) model is the basic security model for privacy. It was designed for multi-user operating systems [10, 11, 12]. The main point with this model is to restrict information from high security level to leak down to the levels with less security.

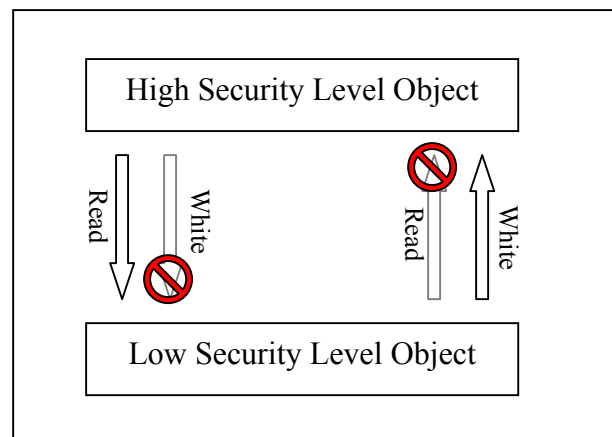
This model of protection consists of the following components:

- Entity/subject (**S**). Subjects can be persons, files, processes or programmes.
- Object (**O**). Objects can be files, directories or subdirectories
- Operation (**A**). The allowed action to be performed on the objects such as access, deny or partial-access.
- Security Level (**L**). The security levels are ordered. Each subject and object is assigned a security level.

L_s = security clearance of subject
(security levels: high, middle, low)

L_o = security classification of object
(security levels: high, middle, low)

S can read from **O** if and only if $L_s \geq L_o$
S can write to **O** if and only if $L_s < L_o$



A subject who has a higher security level can read – down to the object with either equal or lower security level, but cannot write to. Objects with a higher confidential level can never write/append information to objects that has a lower security levels, which means the system (top security level in the system) have the read only access right to all the objects in the entire system. The subjects with a lower- security level can never *read- up* the higher level objects. The subjects with the lower security level can always write or append to objects with the higher security level. Which mean that the subjects with the lower security level have only white and append rights to objects with high security level objects, but do not have enough clearance to read the high security level information.[14].

The problems associated with this model are that it is non-differentiating. Non-differentiation means that all informations belonging to a subject shares the same security level. Thus, no information can ever be passed from a high to a lower level, even if so is wanted. The applications of this models is also restricted to environments with a hierarchical structure.

Other weaknesses is that it does not allow changes in access permission and does not consider the integrity aspect [13].

2.3.2 Biba integrity model

The Biba model preserve the integrity of data belonging to the same 'level'. It prevents high security data belonging to high security environment from leaking to environments with lower security. This model does not concern how data-objects belonging to the same level should behave. Biba model attempts to protect information integrity, complementary to Bell-LaPadula. It is used where the perservation of integrity of data is critical.

There are two properties for dataobjects according to the Biba model:

- The *simple integrity property (SI)*. A subject can have a write access to an object only if the security level of the subject is either higher or equals to the level of the object. Any deviancy from this rule results in a degradation of SI.
- The *star integrity property (*)*. A subject have the read-only access to object o, then it can also have the write access to another object p only if the security level of p is either lower or equals to the level of o.

Note that the read access policy is the same as the Bell- Lapadula model. The difference is that no information from a subject can be passedonto an object in a higher security level. This prevents the contamination of the data of higher integrity from the data of lower integrity.

The major problem associated with this model is that there isn't a practical model because the read and write policies are too restrictive.

2.3.3 Clark-Wilson hybrid authentication model

The Clark-Wilson hybrid model concerns both authentication and facilitates delegation of access rights. Delegation of access rights provides options for situations where several users must all have positive authentication clearance to activate a program that can access certain data.

This model consists of the following component:

- The *subject (S)*. A subject is not allowed to access objects directly.
- The *program (P)*. A program performs predefined actions upon request from a subject upon the objects.
- The *object (O)*. The dataobject being accessed.
- The *transaction (T)*. Every transactions is identified and audited.

The subjects are authenticated and given rights to certain programs. Objects can only be accessed through these programs. Also, both the system and every single transactions must be verified through auditing and certification. The verification feature allows detection of security/integrity breaches.

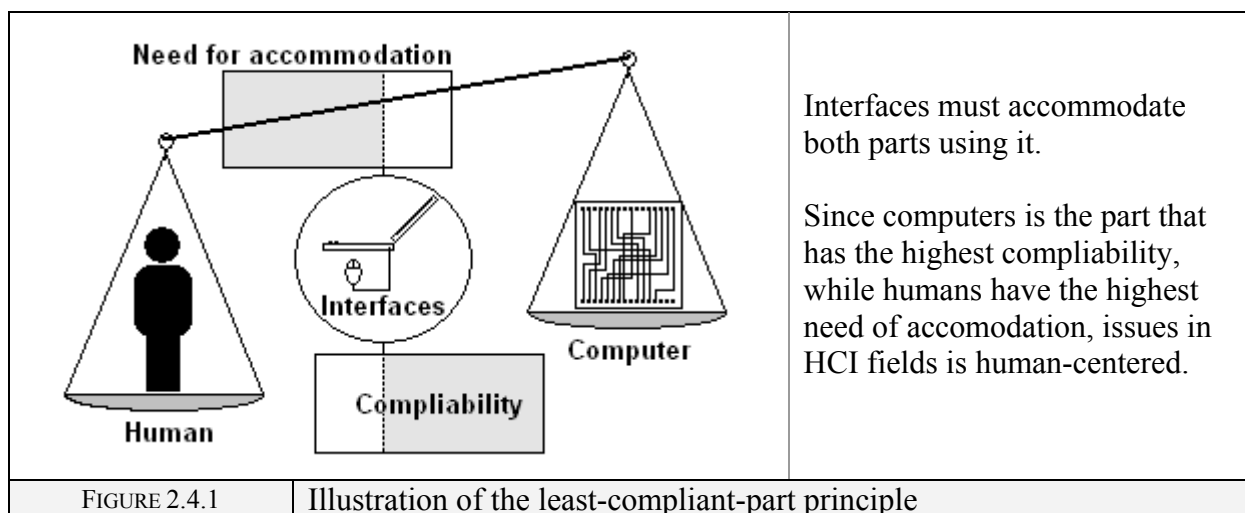
2.4 What is Human Computer Interaction

Computers are designed to serve human needs. At some point - all computing operation requires input from humans, and to some extent - every operation is intended to deliver useful output to humans. If an operation can be divided into suboperations, possibilities for human to interact with the computer system and thus altering the outcome of the dataprocessing arises at every entry and exit points of the suboperations.

The study of Human Computer Interactions helps us to evaluate designs and implementations of computer systems when they are exposed to human interaction.

2.4.1 Human-centered designs

Since humans are the least-compliant part in a HCI-event, the keyword in this field is *human-centered design*. Interactions through interfaces are more well functioning if the interface structure conforms to the least compliant part of the two parties sharing that interface. Since humans neither want, nor are able to, accommodate machines, the system must, to some extent mimic human reactions. That means that a human computer system should be designed so that the operations, as closely as possible, resemble how such corresponding tasks are done from human to human. This typically results in a system with the ability of adapt and react to changes, stores and recognizes pattern from past experience. In certain situations it is desirable to reduce certain performances to harmonize the input-output operations with human limitations.



The HCI examples listed in the following section illustrates the three primary objectives in human-centered design. These three objectives should drive much of designer's, thinking, especially in the earlier stages of interface design.

2.5 The main Human-centered HCI Objectives

Humans are complex and non-deterministic. Many of our non-deterministic aspects, such as our teleological nature - meaning that our goals or behavior may altered during its course, demands elaborate contingency schemes in a interface design. The human-centered design objectives should not only deals with the problems when machines and humans interact, but also should facilitate exploitation of inherent human abilities.

2.5.1. Enhancement of human abilities

This objective dictates that *humans abilities* should be identified, understood, and cultivated.

For example, people tend to have excellent pattern recognition abilities. Therefore the design should take advantage of these abilities; for instance, by using displays of information that enable users to respond on a pattern recognition basis rather than requiring more analytical evaluation of the information [34].

2.5.2. Overcome human limitations

This objective requires that limitations be identified and appropriate compensatory mechanisms devised. A good illustration of a human limitation is the proclivity to make errors. Human are faily flexible information processors which is important, but this flexibility can lead to “innovations” that are erroneous in the sense that undesirable consequences are likely to accur. [8,9]

One way dealing with this problem is to eliminate innovations, perhaps via interlocks and rigid procedure. However, this is asking to throwing out the baby with the bathwater. Instead mechanisms are needed to compensate for undesirable consequences without precluding innovations.

2.5.3. Induce human acceptance

This objective dictates that users preferences and concerns be explicitly considered in the design process. Thus, it is important to ensure that design results in roles that are meaningful to users. In addition, there are other *stakeholders* in the process of designing, developing, and operating as system. For example, the purchaser or the costomer who may not be a user. The interests of these stakeholders also have to be considered [33].

2.6 HCI in File Access Control

Usage of a file access control implementation is complex. It involves handling abstract properties such as ownership, integrity, identification and trust for a large number of objects related to each other in crossed- and multileveled-categories. The objectives described above could be used to help improve the interface of both the UNIX and the Windows models.

A File access control implementation with high Quality of System should have a satisfactory degree of human centered design. That is, it should enhance human abilities, overcome human limitations and induce acceptance as far as possible.

To evaluate whether or not a file access implementation is user-friendly and manageable, we should analyse the most common tasks involved file access control that requires humans input or delivers output to human. We may set up criteria accordingly as to how these tasks should ideally solved from a HCI point of view. These criteria could be tried/measured by means of questionnaires such as those presented in this thesis, resulting in a manageability score.

Chapter 3

Existing File Access Control Implementations

The two most common file access control implementations today are:

- The UNIX Permissions (UP)
- The Windows Access Control List (WACL).

File access control are tightly integrated with their operating system. UP are used by in the UNIX family and different versions of WACL are used in Windows family. There has been bridging attempts in the last years between the two families.

3.1 UNIX Permissions (UP)

A Short history of UNIX:

Three institutions decided to make a decent Operating System together. These were Massachusetts Institute of Technology (MIT), General Electric and AT & T Bell Laboratories. The idea was to build an Operating System that could run on a central computer and the users could logon it through terminals.

The goal was to create a system that could support software development and could manage text. They wanted a system that could also be flexible in such a way that it would offer the same services regardless of hardware. Another demand for the system was to preserve security and resource sharing. The project started in 1965 and was called MULTICS (MULTIplexed Information and Computing Service). In 1969 AT & T and General Electric withdrew from the project, already then the project was too big and complex for it to be useful. MIT completed the project which later turned out to be a huge fiasco.

There is little uncertainty on what the final reason was that led to UNIX creation. The rumor is that the primary reason for UNIX was to make a computer game run on a PDP-7 machine. Others mean that it was a replacement for MULTICS. Whatever the reason, Ken Thompson developed a single user operating system that could run on PDP-7 and named it UNICS (UNIplexed Information and Computing Service). The name was later changed to UNIX (This was in way a joke, but the pronunciation is the same). Later, the C programming

language was created to expand UNIX and make UNIX deployable at other platforms. The first version of UNIX that was written in C was completed in 1973[15].

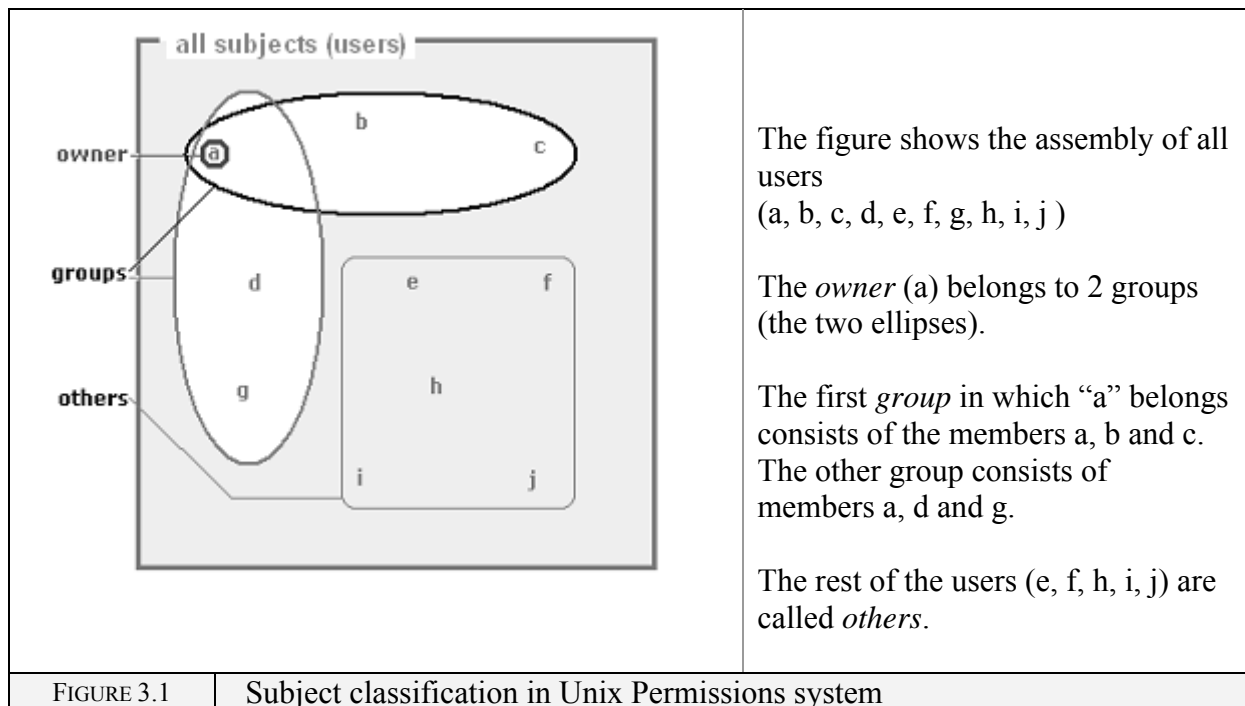
The open source version of UNIX, LINUX, is now possibly even more widespread in use than its predecessor. Price and availability makes LINUX, for many, a better choice than UNIX [16].

UP's Access Right Control Scheme:

Unix Permissions (UP) stems from an older system made in the 70's. The traditional UNIX file system permission model categorizes users into three classes: the *owner class* permissions define the access privileges of the file owner; the *group class* permissions define the access privileges of the owning group, and the *other class* permissions define the access privileges of all users that are not in one of these two classes. (See FIGURE 2.3.1A)

Every file object in the system is associated with three sets of permissions that define access for the owner, the owning- group and for others. Each set contain Read(r), write (w), and execute(x) permissions. This scheme is implemented using nine bits for each object [30, 31].

In addition to these nine bits, the bit *User-ID*, *Group-ID* and *sticky bits* are used for a number of special cases.



Limitations

- A user can only be a member of one group at a time.
- User cannot make their own groups.[17]
- A user cannot give another user special privileges to his own files
- Using UNIX command line to change permissions, you need to know what command and how to use these.

Advantages

- Easy to understand
- Efficient

3.2 Windows Access Control Lists (ACL)

A Short history of Windows:

The trade-name "Microsoft" was first registered with the Office of the Secretary of the State of New Mexico in 1976. IBM needed software and an operating system for its new personal computer.

They struck a deal with Microsoft and in 1981 introduced its Personal Computer, which used Microsoft's 16-bit operating system, MS-DOS 1.0, and other Microsoft products. Microsoft began development of Windows in the early 1980's.

The first operating system utilizing a graphical user interface was used in the Xerox Alto and Xerox Star computers, developed at Xerox PARC.

Apple developed the idea further, and in 1984 they released the Macintosh, which was the first commercially successful computer using a GUI. Microsoft, having landed the profitable deal with Intel, saw the potential of the idea and started development on their own version; Windows.

A year later, in 1985, MS Windows 1.0 was released.

This version of Windows was only a graphical interface to the underlying MS-DOS. This did not change till the released of Windows New Technology (NT) in 1993.

Starting with Windows NT the operating systems had a 32-bit core, not depending on outdated system-calls to MS-DOS. This enabled the operating systems to provide faster, safer, more reliable and more versatile services all the way up to Windows XP, Windows 2003 and the coming Longhorn.

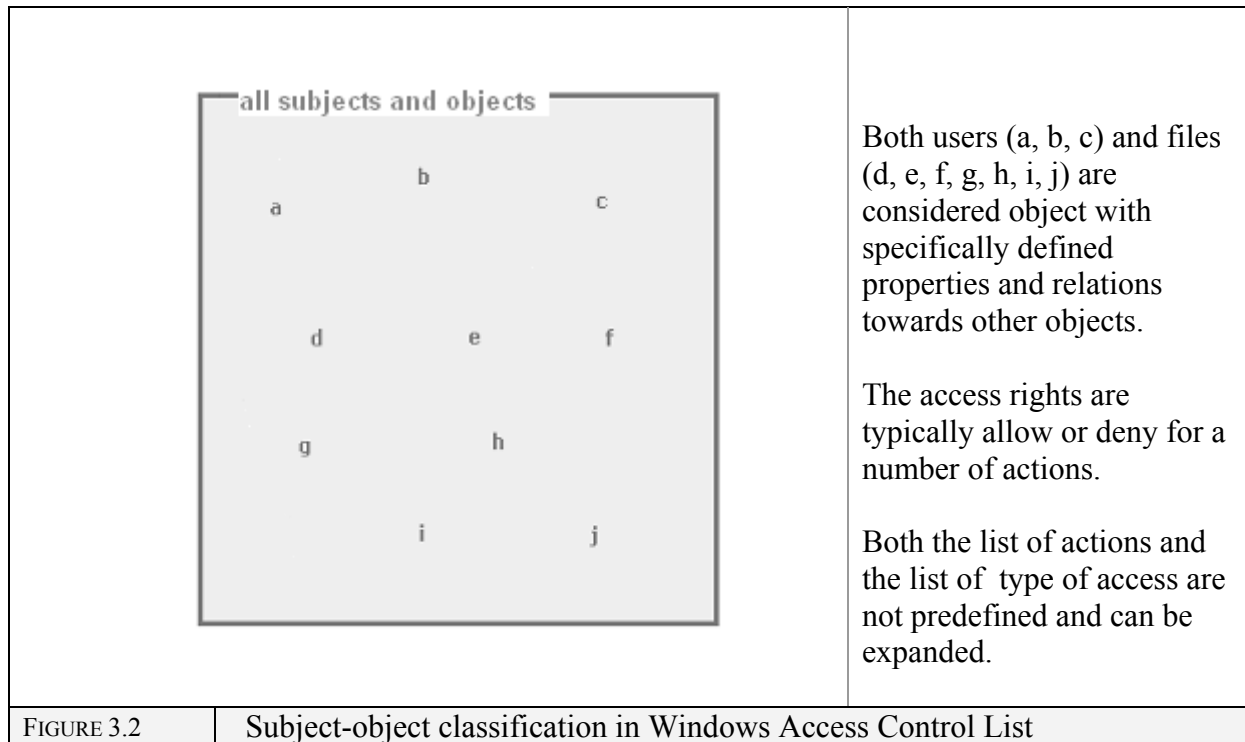
ACL's Access Right Control Scheme:

Access Control Lists (ACL's) is new substitutes for older file access control models and permissions. ACL's can be used for situations where the traditional permissions concept does not suffice. They allow the assignment of permissions to individual users or groups even if these do not correspond to the owner or the owning group.

When talking about ACL, we are talking rather loosely about a family of access permission system. ACL's forms the very basis for Windows security. They alone protect data stored in the system. With the help of ACL's we can define a specific Access right to files for each user-entity. Well known file sharing systems such as NTFS or Novell- Netware use Access Control Lists (ACL's) to control what operations users/ subjects are allowed to perform. For case study, we will select Windows' ACL as it is implemented in Win.XP [18].

Since it is designed for multi-user environments, its popularity is growing with the advance of distributed and networking systems [19, 20].

A standardized version of *ACL* (IP access lists) are used to protect certain areas as Intranets(local network), Firewalls and Internet [26] where we need to control which packets move through the network and where. With ACL it is possible to block traffic from source to destination.[by Joshua Erman, Cisco Access control Lists]. [46].



<p>Limitations</p>	<ul style="list-style-type: none"> -Difficult to understand, because every file system design introduce new attributes with special quality - None synopsis system -Difficult for most users in practically
<p>Advantages</p>	<ul style="list-style-type: none"> -Modern -Possible to specify file the access rights to files for each user individually -Possible to assign users group membership independent to his current group configurations -GUI Simplifies system

3.3 Comparison: WACL vs. UP FAC logic

Although concepts of file access control are similar across the Windows and UNIX platforms, there are sufficient differences in functionality that one cannot substitute UNIX permissions for Windows ACL's (i.e. full emulation is not provided). For example, a Windows application that changes the ACL data of a file may behave unexpectedly if that file resides on a Unix File Server. What is the similarities and differences and between UNIX Permissions and Windows ACL's?

The bellow figure shows, how the computer system translate binary to access rights.

Binary	Decimal	Permissions "rwx"	owner	Group	All others
000	0	777	rwx	rwx	rwx
001	1	755	rwx	r-x	r-x
010	2	644	rwx	r--	r--
011	3				
100	4				
101	5				
110	6				
111	7				

Similarities and differences between WACL and UP

To understand and see clearly the difference between the two systems we can study how the UNIX permissions are translated from Windows ACL.

UNIX file permissions also distinguish between the file owner, the owning group of the file, and other (all other users and group). In addition to the permission modes shown, when translated from the Windows to the UNIX side, all Windows permissions, except read, write and execute, are disregarded. These include delete (D), change permissions (P) and take ownership (O) [21].

UNIX Permission	Windows ACL's
r--	Special Access(R)
-w-	Special Access(W)
--x	Special Access(X)
rw-	Special Access(RW)
r-x	Read(RX)
-wx	Special Access(WX)
rwx	Special Access(RWX)

When mapping to UNIX file permissions from ACL, it is not possible to add new ACL entries because only the *owner*, *owning group* and *other* ACL entries are supported by UNIX permissions. UNIX ignores unrecognized entries. Conversely, we cannot delete any of the three entries listed above as these entries are required by UNIX.

Windows has a default file right which automatically applies to files which created on local file-stores. The owner of the file will automatically have full control of the file. Which means the owner of the file gets all rights when a file is created in a folder in his or her DFS file-store. When a file is created in UNIX on the other side, it starts off by being "all denied".

Both systems do include some default “categories” in their model. UNIX categorizes the user according to the coarse relation to the owner of the file, (self, group and other), while ACL divides user according to roles as viewed from the administrators view point (administrator, sub-admin, user, guest).

Windows ACL’s allow one to set permissions with finer control that does the Unix file mode. For example, one can allow a user to append data to a file as opposed to overwriting the file, something which is impossible to do with Unix. ACL’s also allow one to permit specific users to change the permissions on a file. In the nutshell: the biggest difference is that ACL’s allow us to accord permissions on a user-by-user basis, rather than the three categories of users permitted by UNIX file systems.

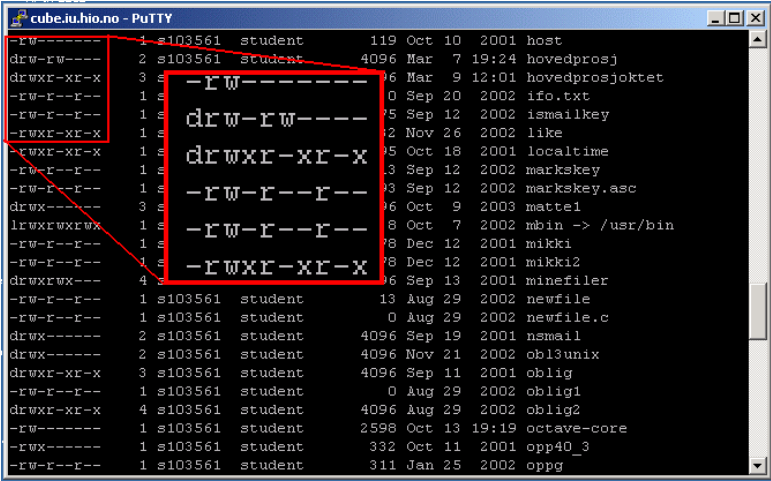
Windows ACL’s may be applied on for applications/process. It is possible to set access control on specific applications.

ACL’s is amongst other things better suited than Unix permissions to define ownerships. [22] The control of Windows ACL’s, as with many of other Windows-based applications, has been simplified by a graphical user-interface, and many common settings are made default. Still, when coming to the more complicated settings, correct use demands great deal more understanding from the view point of the normal user. For many reason we later will discuss, users are often more uncertain when dealing with ACL [23].

3.4 Comparison: WACL vs. UP User Interfaces

3.4.1 UNIX User Interfaces

The following figures show how settings of access rights can be manipulated by the command line and a graphical user interface in the UNIX system.



```

cube.iu.hio.no - PuTTY
-rw-rw---- 1 s103561 student 119 Oct 10 2001 host
drwxr-xr-x 2 s103561 student 4096 Mar 7 19:24 hovedprosj
drwxr-xr-x 3 s103561 student 0 Sep 20 2002 ifo.txt
-rw-r--r-- 1 s103561 student 75 Sep 12 2002 ismailkey
-rw-r--r-- 1 s103561 student 72 Nov 26 2002 like
-rwxr-xr-x 1 s103561 student 75 Oct 18 2001 localtime
-rw-r--r-- 1 s103561 student 3 Sep 12 2002 markskey
-rw-r--r-- 3 s103561 student 73 Sep 12 2002 markskey.asc
drwx----- 3 s103561 student 76 Oct 9 2003 matte1
lrwxrwxrwx 1 s103561 student 8 Oct 7 2002 mbin -> /usr/bin
-rw-r--r-- 1 s103561 student 78 Dec 12 2001 mikki
-rw-r--r-- 1 s103561 student 78 Dec 12 2001 mikki2
drwxrwx--- 4 s103561 student 76 Sep 13 2001 minefiler
-rw-r--r-- 1 s103561 student 13 Aug 29 2002 newfile
-rw-r--r-- 1 s103561 student 0 Aug 29 2002 newfile.c
drwx----- 2 s103561 student 4096 Sep 19 2001 nsmail
drwx----- 2 s103561 student 4096 Nov 21 2002 obl3unix
drwxr-xr-x 3 s103561 student 4096 Sep 11 2001 oblig
-rw-r--r-- 1 s103561 student 0 Aug 29 2002 oblig1
drwxr-xr-x 4 s103561 student 4096 Aug 29 2002 oblig2
-rw----- 1 s103561 student 2598 Oct 13 19:19 octave-core
-rwx----- 1 s103561 student 332 Oct 11 2001 opp40_3
-rw-r--r-- 1 s103561 student 311 Jan 25 2002 oppg
                    
```

The owner, group, and other user classification is shown in the first column.

Example from line 3:
“d rwx r-x r-x”

d = this entry is a catalogue/folder


rwx = the owner has all permissions (read, write and execute access for the owner)

r-x = read and execute access for the group class

r-x = read and execute access for the other class

FIGURE 3.4.1A

Output from UNIX command line for access rights control



Class	Show Entries	Write Entries	Enter	Special
User	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/> Set UID
Group	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/> Set GID
Others	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/> Sticky

This is the graphical equivalent of figure 2.3.4A

By clicking, one can set rights for the entity classifications users, groups and others.

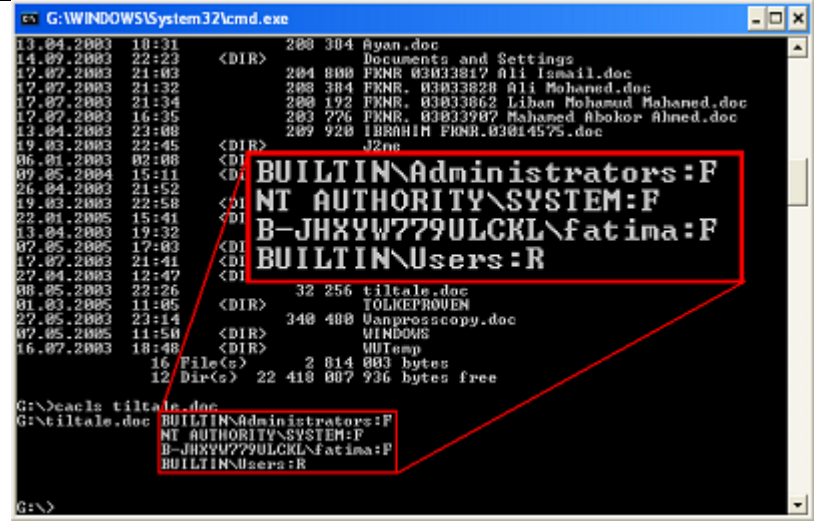
The special rights user-ID, group-ID and sticky bits are on the rightmost column

FIGURE 3.4.1B

UNIX GUI for access rights control

3.4.2 Windows User Interfaces:

The following figures shows how settings of access rights can be manipulated by the command line and a graphical user interface in the Windows system.



The screenshot shows a Windows command prompt window titled 'G:\WINDOWS\System32\cmd.exe'. It displays the output of the 'icacls' command for the file 'tiltale.doc'. The output lists the permissions for various users and groups, with a red box highlighting the permissions for 'BUILTIN\Administrators:F', 'NT AUTHORITY\SYSTEM:F', 'B-JHXYW779ULCKL\fatima:F', and 'BUILTIN\Users:R'. Below this, the permissions for the file itself are shown as 'BUILTIN\Administrators:F', 'NT AUTHORITY\SYSTEM:F', 'B-JHXYW779ULCKL\fatima:F', and 'BUILTIN\Users:R'.

The system administrator has full control (F) of the file in question.

The operative system (NT Authority\System) has also full control.

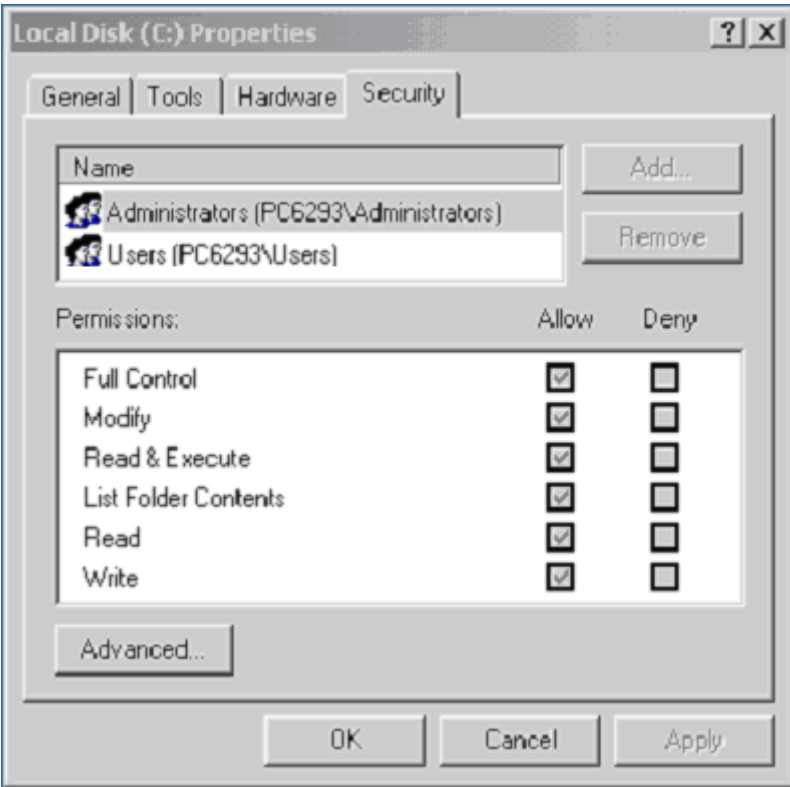
The user (fatima) also has full control.

Other users only Open , read the file or execute program (R)

The file in question “tiltale.doc” full control.

FIGURE 3.4.2A

Output from Windows command line for access rights control



The screenshot shows the 'Local Disk (C:) Properties' dialog box with the 'Security' tab selected. It displays a list of user objects with access relations to the object: 'Administrators (PC6293\Administrators)' and 'Users (PC6293\Users)'. Below this, a table of permissions is shown with 'Allow' and 'Deny' checkboxes. The permissions listed are Full Control, Modify, Read & Execute, List Folder Contents, Read, and Write. All 'Allow' checkboxes are checked, and all 'Deny' checkboxes are unchecked. An 'Advanced...' button is visible at the bottom left of the dialog box.

The object is here the disk c:

The upper list view shows the user objects with access relations to the object

The predefined 7 types of permissions are listed below.

Allow and deny check boxes determine the Permissions granted to user.

- If neither box is checked, the user is not allowed that right.
- If the allow box only is checked, the user is allowed that right
- If the deny box is checked, the user is always denied, even when the allow box is checked

The Advanced button leads to less frequently used configurations [25].

FIGURE 3.4.2B

Windows GUI for access rights control

Chapter 4

Methodology

4.1 Research planning

The first place to seek for up-to-date information about file access system performances and security issues is the Internet. We started by collecting information from selected websites, especially from published research papers in ACM and IEEE , and from forums dedicated to answering problems regarding file permissions and related security problems. These websites discuss the most common problems and possible countermeasures. The frequency of which a certain problem is mentioned serves as an indication on how serious that problem is.

However, the evaluation of the preception and experience of users on the different file systems are not sufficient and needs to be addressed. We will therefore in this chapter define our research questions, method to be used including recruitment of study subjects and the tools to be used. We will also summarize the statistics we will use in order to describe our study variables.

4.2 Research questions

We have formulated the following research questions:

- Is there a difference between UPand WACL file access systems
- Is UNIX permission easier to give/change an file access rights than Windows ACL
- How useful is file access controls for the users
- How important is the default access file rights for system users
- How is the knowledge on file access control among users
- Is there any correlation between gender and the preference of operative systems
- Does age mean any thing for the security

4.3 Research Material

We are planning to undertake study on file access control systems among students and staff at the Oslo University College Department of Engineering (OUCDE). We will use two separate questionnaires in order to collect relevant information. This study will be undertaken a period of two weeks in February 2005 at OUCDE.

Selection of participants: 100 voluntary persons at OUCDE will be asked if they are willing to participate the study. The study consists of two parts.

Study I: A group of students will be recruited from computer labs, while teachers will be approached at their offices and ask if they are interesting to participate the study.

Study II: Another group of students who have sufficient knowledge of computers will be recruited for more technically demanding questions.

The inclusion criteria will be a minimum knowledge of computer. Therefore we have decided to include only for those who were at computer department. It is planning two weeks for data collection. Those who fulfil the criteria and agree on the participation will be asked to fill in questionnaires. To economize the study participants each participant will be given an ID number.

In addition to those described above, we also interview to system administrators in the department (See 5.5.3).

4.4 Questionnaires

A detailed questionnaire (Study 1) has been developed and will be used in order to collect the background information of the participants such as *gender*, *age*, their knowledge of computer and length of *computer experience*. The questionnaire was formulated as pre-coded with dichotomous-variables¹ (yes or no) [27, 28].

Another questionnaire (Study 2) was developed for in-depth analysis and will be asked to fill inn by selected persons (not the same as above) through interactive web pages.

Two other persons (experts) will also be interviewed orally. These two have a first hand experience on file systems and therefore could provide indepth respons on which of the two systems are easy to administrate.

¹ dichotomous- variables means that you can only answer “ yes or no” to the question

4.5 Control of data and statistics

4.5.1 Tools to control data and statistics

Data processing and statistical analysis will be preformed using the Statistical Package for the Social Science for Windows (SPSS). The categorical values will be presented as percentages. Spearman's correlation coefficient will used to see if any correlation exists between dependent and independent variables such as the preference of the two Operating systems and gender.

Probability values > 0.05 will be considered as significant (see 5.6.1).

4.5.2 Ethical issues

The researcher explained the objectives of the project and the participants understood that their participation was optional and they could quit at in any time during the interview. After that they provided their consent.

The participant's identity was anonymous and therefore their names or date of birth were not asked, but we have to know their age. While processed the data each participants was given an ID number.

4.6 Procedures

Answers from the questionnaires were put in a statistical analyzing Software program called SPSS. This program helped us to organize data attained from the questionnaires before analyzing them.

The following procedure was used for controlling data and to avoid stochastic human error. Each submitted form was given its own number in the range of 1-63. After that every single question was also given a code number (for ex. 1, 2, 3). The variables were also coded (for ex. yes=1, no= 0, both = 3, don't know = 4).

Finally the process was controlled twice by two other people with experience in SPSS before data was further analysed.

It is important to point out that the results we have presented here are based only on the responses from research subjects.

4.7 Research subjects

The group of persons that best can affirm our research questions are people that have daily contact with computers that is people in academic pursuits or employed in commercial enterprises.

We have chosen to focus on students and teachers at Oslo University College for the simple reason that they are readily available. Part of the information gathering is through questionnaires on the web, and partly handed out and answered under supervision. There were also conducted 2 special in-depth interviews with system department network administrators of the college. The statistic materials were collected on a medium selection of randomly encountered students and teachers.

The total number of participants amounted to 92 persons. The goal was to have 100 respondents to get a sufficient number for statistical significance.

Students and teachers

There were 63 respondents out of 65 asked on study I and 27 respondents out of 40 asked on study II.

The average age of participants was 30 years in study I.

Participants had an average of 5 years experience in computers in study I.

The participants of study I 32 % were women and 68 % were men.

Among those who answered study I 72% were students and 28 % were teachers

The participants of study II; were all male students, they all have minimum 5 years computer experiences. (See the tables below for more details.)

Experts

Two other persons (experts) were interviewed in-dept in study III.

Both subjects were system administrators at Oslo University College. They expressed sincerity to give complete answers. Both were presented with the same questions, where they told about their experience and views. Each oral interview was 15 minutes in duration. The questions asked were formulated as broadly as possible.

Subject 1 had responsibility for the Novell Netware (Windows) used by the school to provide file sharing, in which file access control is a major part of daily maintenance routines. Since Novel Netware uses windows ACL, his experience should provide us with a true picture on how well ACL works in practice.

The subject had more than 10 years experiences as system- administrators, and also had advanced knowledge of UNIX permission, enough to provide us with a qualified, well-grounded answer about personal preference.

Subject 2 had responsibility for the UNIX part of the schools network. His expertise was therefore in the area of UNIX permissions. He had 6 years experience as system-administrators.

Summery of the participants in **study I**

Gender	Total	Average age	average data experience	Students %	Teachers %
Men	68 %	30 years	5 years	72%	28%
Women	32%				

Summery of the participants in **study II**

gender	Average age	average data experience	Students %
Men	30 years	5 years	100 %

Summery of the participants in **study III**

Gender	Average age	average data experience	Position
Men	42 years	25 years	system administrators

Chapter 5

Results and Analysis

In this section we will show the results from the questionnaires. The answers will be presented in a descriptive way. It is important to note that the results from questionnaires in study II will be used as supplementary to results from study I. These because the results from study II are quite similar to the results from study I. We have therefore found it reasonable to present the two data sets as aggregated data, which mean we can use Study I result to fortify our assertion.

5.1 Definitions and Hypotheses

Complex systems such as a file access control implementations has compounded quality. Following is a set of factors and relations that are likely to contribute to the overall quality of system. The proposed relations can be considered as work hypothesis, and results arrived by using these hypotheses can be confirmed by comparison against measurable quantities from tests.

Definitions:

D₀: The Quality of System (Q) for any system implementation for a chosen group of users is defined as the sum of the subjective *user-experience* (Q_E) and the *objective technical* part (Q_T). Q is between 0 and 1. A large value of Q means that the system is better.

Formula F₀

$$Q = Q_E + Q_T, \quad (0 \leq Q \leq 1)$$

D₁: The subjective user-experience (Q_E) is the weighted sum of the addends usefulness (Q_u) and manageability (Q_m).

Formula F₁

$$Q_E = \alpha Q_u + \beta Q_m$$

D₂: The manageability of a file access system (Q_m) is the weighted sum of that systems understand ability (Q_n), user-friendly for users (Q_o) and user-friendly for administrators (Q_p).

Formula F₂

$$Q_m = \beta_1 Q_n + \beta_2 Q_o + \beta_3 Q_p$$

D₃: The objective technical quality (Q_T) of a file access system is proportional to compliance to the rules set by the chosen security model (Q_s). λ is the proportionality constant.

Formula F₃

$$Q_T = \lambda Q_s$$

D₄: The overall Quality of System (Total quality) for a file access system for a given user group is thus defined as:

Formula F₃

$$Q(\text{user}) = \alpha Q_u + \beta_1 Q_n + \beta_2 Q_o + \beta_3 Q_p + \lambda Q_s$$

Hypothesis:

H₀: We postulate that there is a difference in the Quality of System (Q) between UNIX and Windows files access systems.

Formula F₄

$$(Q_{\text{unix}} - Q_{\text{windows}}) \neq 0$$

H₁: We postulates that if two file access implementations are released simultaneously in a free market* and have existed for approximately the same period of time, the system with the highest Quality of System will also have the highest popularity percentage/market domination(P)

Formula F₅

$$Q = P, \quad (0 \leq P \leq 1)$$

H₂: We postulates that the weighting of the Quality of System for a file access implementation between two user categories is most accurate when the weighting is determined by the exposure-weighted value (E) (how often the files are accessed) of each groups multiplied by the amount of disk size (Z) allocated to that group in a normal situation.

Formula F₆

$$Q_{(o+p)} = \beta_2 Q_o + \beta_3 Q_p = (E_o \cdot Z_o) Q_o + (E_p \cdot Z_p) Q_p$$

After developing this model showing above, we were not able to use it for due to the quality of responses and time constraints.

5.2 Strategy matrix

The plan was originally to evaluate the results with respect to the formal model in section 5.1. The Quality of System is then given by $Q(\text{user}) = \alpha Q_u + \beta_1 Q_n + \beta_2 Q_o + \beta_3 Q_p + \lambda Q_s$, where the contributing quantities may be determined as listed in the matrix below.

Criterion for a good File Access Control implementation	Unix permission	Windows ACL
Usefulness (Q _u)	76/100	76/100
Understandability ** (Q _n)	47/95	17/95
User- friendliness* (Q _o)	82/100	0/100
Easy administrated (Q _p)	0/2	2/2
secure system (Q _s)	76/100	76/100

- for single user (common tasks)*
- for experts users (more then common tasks)**

Ideally we would like to measure α , β_1 , β_2 , β_3 and λ , but this is not possible here now (see section 6.1.9).

5.3 Analysis of results from study I and II

5.3.1. Description of variables

In the two questionnaires we have a total of 38 questions to determine the usefulness score of the two systems and how users value the two systems with respect to manageability. We have decided to group them in to five main categories as following:

- **Group1: Preferences;** which Operating system users prefer to use daily.
- **Usefulness;** Measures the usefulness score of common file operations(Group 2)
- **Knowledge;** Test questions about knowledge of ACL vs. UNIX permission(Group
- **File right management knowledge;** Knowledge of file access management (Group 4)
- **Security** (Group 5)

In addition to those five groups we will also analyze if there are any correlations between the parcipants gender and preference of operative systems, we will also do the same for parcipants age and security.

5.3.2 Group 1: Preference

1. What operating system do you use?

Result:

- 16 % Unix
- 70 % Windows
- 13 % uses both Operatin systems
- 1 % didn't answer question

The participants were asked if they use UNIX or Windows Operative system. 16 % and 70 % replied that they use UNIX and Window daily respectively, while 13 % use both of the systems.

We can tell from the questionnaire that Windows is the more popular choice of operating system, while the general knowledge of UNIX among these users seems fairly high.

This could be interpreted as an indication that, to some extent, Windows is used, regardless of the knowledge possessed by the user.

It must be noted that this only mirrors the results the of given questionnaire, and is not necessarily valid in reality.

2. Is there a big different between UNIX and Windows file access systems?

Results:

- 32 % said yes, there are big differences between the two systems
- 21% said no, there are not differences between the two systems
- 43 % did not know the difference between the file systems
- 4 % did not answer the question

3. Which system do think is easiest when changing file permissions?

Results:

- 48 % said Unix is file access system is easiest
- 18 % said ACL's file access system is easiest
- 27 % do not know which of the two systems is easiest
- 7 % did not answer the question

9. What command do you use when you want to list files og catalogues in DOS-command window?

Results:

- 27 of 27 asked says we do not know

32 % of the participants responded that there is a big difference between the two systems when asked if such differerce exist, while 21% replied there are not big differences between the two systems.

The participants were also asked which of the two systems is easiest to maintain and 48 % replied that UNIX system is an easier system than ACL, while 18 % replied that ACL is the easiest system. It is also worth to report that almost 32 % did not answer the question.

From the results we can see that the most of the participants do not know the difference between the two file systems. While most of the participants find the UNIX file system the easiest one to use.

We can see that the most of the participants have knowledge of UNIX Permissions and lack of knowledge about Windows ACL. That might explain why the participants find ACL difficult to use.

5.3.3 Group 2: Usefulness

4. Do you open more than 5 files daily?

- 95 % open more than 5 files daily
- 5 % says no

5. Do you save more than 5 files daily?

- 67 % save more than 5 files daily
- 23 % says no
- 10 % did not answer the question

6. What do you prefer: work from home or at the school?

- 46 % of participants work at school
- 40 % work at home
- 14 % both places

It was also interesting to know how many files the users save on the systems and open per day. Almost 67 % of the participants replied that they save more than 5 files per day while 95 % open 5 files or more per day.

On the other hand we can see that 46 % of those 63 respondents prefer to work at the school.

40 % prefer work at home and 14 % work at both places. We find logical that those who choose to work at the school have indeed store documents with sensitive contents on publicly accessible areas of the network. Because of this they will need the ability to change file access properties (more about this in the next box).

7. How do you save electronic documents then?

- 64 % save sensitive documents in network system at the school
- 34 % don't do that (see next question)
- 2 % did not answer the question

34 % show above save in several different ways as:

- 15 % removable media (CD, USB, floppydisk)
- 16 % removable media + harddic (local)
- 3 % harddic + sharind areas (as a cube)

8. Do give your folders and files meaningful names (recognizable name)?

- 91 % say yes they do that
- 9 % say no they do not do that

It might be possible that many users save confidential information in the network system without knowing the needs for protection while saving files in common areas. The participants were asked if they save sensitive documents in the system and 64 % responded that they save sensitive documents in the system while 34 % do not do that.

This is a clear indication that setting file access rights is necessary in order to save their work and documents safely. We know from question one, preference of operating system, that most users regularly work with Windows. Additionally question ten and eleven shows that the knowledge of Access Control Lists is rather low, 59 % does not even know what ACL, the file access system of Windows is while 40 % do not know how ACL's is works, in other words they can't nor use it.

Combined with the high percentage of participants storing sensitive documents in publicly available areas, this means there could be a lot of unprotected, sensitive files on the shared network or similar.

A related issue we have included in the questionnaire whether people give their folders and files meaningful names such as "Solution to mandatory assignment 1.doc". If this is the case, gaining access to these documents could be interesting for several other students, something the college would try to avoid by having the proper file access rights set.

As much as 91 % replied that they give their files and folders meaningful names.

5.3.4 Group 3: Knowledge

9. Do you know what is the differences between Unix and Windows file Access rights?

Results: table 1

- 52 % responded that they know the difference between two systems
- 46 % didn't know the difference between the two file access systems
- 2 % did not answer the question

To the question about knowing the difference between UNIX and Windows file access rights 52 % replied that they know the difference between two file access systems while 46 % do not know the difference between these two systems.

From the result we can draw a rough conclusion that half of the participants can not see any difference between MS Windows and UNIX file systems. Further it is difficult for the participants to see the difficulty level between the systems when participants do not know the difference between the systems.

10. Do you know what an ACL is at all?

Results:

- 59 % have not heard about ACL's
- 37 % have heard what ACL's is
- 4 % did not answer the question

11. Do you know how ACL works/ function?

Results:

- 27 % know how ACL's works
- 40 % do not know how ACL's is works
- 33% did not answer the question

The participants were also asked if they know what ACL is 59 % responded that they have not heard about ACL's while 37 % said they heard about ACL's. On the other hand 27 % replied that they know the function of the ACL system and 40 % do not know how the system functions.

We can see from the results that most of the participants have never heard of ACL file system. But among the participants who knew about ACL do not know how it works. Further there are 1/3 of participants who did not answer the question which we could conclude with that they did not know about or have never heard about ACL.

We can conclude with that there is lack of knowledge among the participants about the ACL file systems.

5.3.5 Group 4: File right management knowledge

12. Did you ever need to change or specify file rights and not succeed?

Results:

- 16 % had encountered problems while setting file access rights
- 83 % had not encountered problems
- 1 %

The participants were asked if they had ever encountered problems while attempting to set file access rights. There were 16 % who responded having difficulties, while 83 % had not.

Due to answers from study II we believe that the general knowledge of ACL is very low, and thus the low percentage of participants having faced problems while setting file access rights is mostly valid for the UNIX system.

(The question could have been phrased differently; in particular it would have been interesting to know whether the answer would be the same with regards to both UNIX and Windows. Additionally the question should in fact have been two; "Have you ever needed to specify file access rights?", and "If so, have you faced problems doing so?")

13. Do you know how to change file rights?

Results:table 1

- 80 % know how they could give others file rights
- 20 % didn't have that knowledge

7. What does this mean: rwx rw- r--?

Results:

- 11 of 27 sked says we do not know

What do command umask do?

Results:

- 19 of 27 asked says we do not know

The participants were asked if they know how they can give or deny others(a friend) file access rights and 80 % said that they could do this while 21 % couldn't do this by themselves.

Given the response to question10 and 11 regarding File Access Lists, we must interpret the vast majority who know how to give access rights are referring to the UNIX file access system.

14. Do think it is usefull to file access rigths?

Results:

- 76 says % said is of changing of file access rights useful
- 22 % said it was not so important.
- 2 % did not answer

It was also interesting to find out how was the usefulness of changing of file access rights for users and 76 % said changing of file access rights was very useful while 22 % said it not so important.

We can conclude from the results that most of the participants think that it is important to change file access rights. I believe that they want to do so to, protect their files and make it private. The problem is that they do not know how to use the access control systems. We know that 70% of the users use windows daily, among those users almost 60 % don not know what ACL is. And therefore we can conclude with that practically they can not protect their data files (we rest on our assertion on next question).

15. Do you change file rights or you just use default file rights in the system?

Results:

- 76 % use default file access settings
- 22 % do not use default file access settings
- 2 % did not answer

The participants were asked if they use the standard file access rights as suggested by the system administrator. There were 76 % who said they do not change the default file access rights while 22 % replied they change the default file access rights to satisfy their own personal security policy.

We can see from the result that many users did not change default value*. This value is different from system to system, because it is regulated from system administrators. What we understand from the result is that system administrators must consider a lot when deciding this value which will be wanted to be standard for the system users. Since many users use default file rights we recommend that the default value must satisfy a maximal demand of security.

5.3.6 Group 5: Security

16. Have you thought that the others can copy your documents?

Results:

- 76 % were aware of security matters
- 24 % didn't think about the issues

The participants were asked of their awareness of security matters of the documents and the possibility that their files will be available for unauthorized persons. As much as 76 % replied that they are vigilant and aware of the security matters and take therefore the necessary steps in order to avoid the security weakness, the other 24 % don't consider about the issues at all.

In addition of that nearly every participant leaves workstations while logged on although they take into consideration to issues concerning the safety of their sensitive files.

This leads to concluding that while aware of the safety issues regarding sensitive files, many do not actually care to do anything about it – even if they know how (we rest on our assertion on next question).

17. Did you know that you can protect your files with password

Results:

- 83 % knows about password protection
- 15 % didn't know that
- 2 % did not answer the question

*Default value are the value that gives when user create a new file or folder

We want to know the knowledge of the participants on protecting files for using of password. So 83 % replied yes for having the protection of files with password while 15 % said it is not possible.

While it is impressive that as much as 83 % know of password protection of files, it would be far more interesting to see whether the participants knew how, and in what applications this is possible.

It is for instance not possible with regular UNIX files, but applications such as MS-Word and Acrobat reader offer password protection of their respective document types.

18. Have you ever take a break, leaving your console open to others?

Results:

- 92 % take break while on logging in the system
- 5 % say no they don not do that
- 3 % did not answer the question

It has been observed that some users leave the computers unlocked and therefore exposed the systems to danger. We therefore want to know the frequency that users leave the computers without log off the system. 92 % of the participants replied that they take break often while log on the system.

Most likely failing to log out from the system when taking a break or similar is caused by fear of not being able to regain the computer when coming back. If there are more potential users than available computers, this can be understandable.

A possible solution is to offer the option of locking the workstations, effectively “reserving” the computer while you are gone. This however is often not available, due to the possibility of too many computers being locked without a user present. Additional users would then find a near-empty room, with no available computers still.

Other possible reasons could be being too lazy to log back in, not reading company policies regarding security and staying logged on to workstations.

In either case having the system automatically log a person out after a given number of minutes without activity would help, but ideally people would log out when leaving a workstation to avoid clogging resources, as well as not posing a security risk.

We believe that with such a high percentage of the participants leaving their workstations while logged on, several of these know the risk it poses but ignores the threat.

In hindsight we see that this is an additional question that should have been added to the questionnaire; “If you do leave the workstation without logging out, what are the reasons for this?”

19. Would you like to recommend others users to change their file rights?

Results:

- 49 % that they will advise to other users on protection of their files
- 47 % responded they would not do that
- 4 % did not answer the question

The question of recommending to other users on the protection of their files responded 49 % that they would give advise to other users on protection of their files in order to change the file rights while 47 % responded they would not do that.

5.4. Factors affecting the preference of operative systems

We have analysed some factors which we thought they will influence the use preference on file systems. These include gender, age, work place, experience and status. We will only describe here for the factors where correlations have been found.

Correlation between gender and preference of operative systems

Results: table 1

Women

- 5 % uses Unix
- 90 % uses Windows
- 5 % not answered

Men

- 20 % Unix
- 60 % uses Windows
- 18 % uses both

It is interesting to find out whether there is a correlation between gender and the use of UNIX and ACL Windows among the users. We have tested this statistically and found that there are significant difference, which means there are more women who prefer to use Windows than men ($p=0,01$).

This means that 90 % (18 of 20, were $n^2=20$) of women prefer to use Windows against 60 % of men (26 of 43, were $n=43$). There was also a significant difference between men and women on the preference of UNIX ($p=0,05$), which means that there were only 5 % of womans who prefer the UNIX Operating system while 20 % of men perefere UNIX Operating system.

² n is the number who participate the reseach

5.5 Factors affecting the security of file systems

Does age have any impact on security of file systems?

Result: table 1

- 40 % of those who are under 30 years will advise to other users to protection their files
- 60 % those above 30 years will not recommend other users to protection their files

We have tested whether age can explain the awareness of system security but could not find any such correlations and therefore we have divided the age into two different age categories. After that we have observed a tendency that the younger users are more aware of system security than the older users. This means that 40 % of those who are under 30 years of age will not recommend to others to change their file access rights, while 60 % of those above 30 years would not recommend it.

From the above results we can conclude with that the younger generation of computer users are more aware of computer security then the older generation.

Chapter 6

Discussion

6.1 What makes file access system good ?

File access systems are made to control file access for both machine-to-machine interaction and for human-computer interaction. File access control systems (FACS) are designed mainly for data transactions such as networking communications and still needs to be configured by human users. The quality of FACS must therefore accommodate both subtle human aspects and purely technical ones [102].

In this research we are not discussing the aspects regarding the costs of using WACL and UP since file access systems are integrated into their existing operating environment. If the system is difficult to use however, certain overhead costs could be calculated due to unnecessary time spent trying to set file rights or similar.

6.1.2 Security weaknesses

The issue is concerning people's habits. It can be understood in various ways; both negative and positive. For instance some people will have a habit of always setting new files as read-only, while others will do the opposite; having new files both read and writeable.

The possible mistakes people make when using a multi user system and not change his or her file rights, what happen then is that every one can access her documents and do what every their wish. If she is connected to a network and have some directories/files which contents her or his nice pictures/drawing and document she or he want people to see only, but not change or modify, then she do not have a chance to control that if she or he is not even knowing how to do that. This of course depends on the operating system the person using. We will try to point out some of those typical mistakes:

- Giving wrong file permissions, e.g. 777* instead 755* or 644* (UNIX)
- Deleting important system files (execute scripts)
- Change important system files, which can cause harm to system (see table i 3.3)

*644 = read and execute access rights to owner, and read to group and all other users

*777 = all access rights to owner, group and all other users

*755 = all access rights to owner, group and others have read and execute

6.1.3 Technical quality

In this particular thesis we have compared UNIX Permissions with ACL's in relation to the users understanding of the context / meaning. We have also evaluated the technical solution behind the two different systems.

Both systems have from a technical point of view been taken into consideration of the four security-modules we have described earlier in the background chapter. These modules have originally been created /invented for military purpose (*very strict rules*) and therefore none of the two systems can use them directly. But the file access control systems use the same basic ideas concerning the idea of protecting information and data in a proper / satisfactory way. However, we are still missing the fifth element namely user experiences on file access control systems which is equally important and needs to be addressed.

In this thesis we will then highlight the importance of user experiences on file access control systems. Although technical solutions behind these systems are satisfactory, still it is not good enough, if users can not utilize the tools because they don't understand the systems.

In this discussion we will emphasize on the users knowledge about the file access systems, and we will try to see the experience and perception of user experience of the two systems.

6.1.4 Method

The original plan was to collect the data through interactive web pages* to save processing time and to recruit more participants for the study. But we have later realised that the method was not effective due to some limitations such as the required effort from the participants and time demand.

In order to recruit enough people for the study, we have therefore decided to recruit students from computer labs and teachers from their offices. We recruited enough participants and the response rate was firmly high and therefore we assert that the recruited participants are representative for the project aim and fulfilled our inclusion criteria.

However, a selection bias could have been aroused when the study participants were recruited so that the study sample differs systematically from the population from which it was meant to represent. To ensure a better degree of control, we conducted the questionnaires under supervision. The forms were handed out direct to the students and teachers. Each person was given the time he needed to complete the questionnaires; the range of time used was from 12 to 34 minutes. The presence of a supervisor has also been a positive effect and increased the quality of the answers.

Since there are many unknown factors contributing to how a system functions, the easiest way to determine what system is most successful is using *series of questionnaires*. We started by

using a simplified, general questionnaire where we propose some factors that are most likely to have great impact on system performance*. ³From this preliminary results we get some idea of the sorts of problems a user encounter daily, what the user like with a certain system, what he think is difficult or awkward. We then starts on the second round, where we are able to formulate more specific questions(study II) that will give us the final answers. The second part of the research will also be aimed at a selected group of respondents. Some of the forms were later returned to the participants, in order to finish their answers; for instance the question of operating system preference was omitted by some participants.

6.1.5 Test participants

The group of people that best can affirm our research questions are people that have daily contact with computers that is people in academic pursuits or employed in commercial enterprises.

We have chosen to focus on students and teachers at Oslo University College for the simple reason they are readily available. Additionally these subjects have a background that should enable them to answer such questions without difficulties.

The two respondents from survey 3 are especially qualified to answer comparison questions between UP and WACL since they have daily contact with UNIX and Windows operating systems.

6.1.6 Participant knowledge

The questionnaire results show a surprising low average level of knowledge on the Windows ACL model, which also was the most used operating system among those who participate the reseach.

The reasons for this could be many. One possibility is that the test subjects did not feel an urge to insert any effort into answering the questions.

6.1.7 Questionnaires

In the beginning we were asking the participants general and easy questions, and then gradually we were increasing the complexity- level / difficulty – level.

What we found most interesting was that almost everybody would answer all the questions, even if they were unsure / insecure about what they were going to answer.

Our mistake was that we formed the questions before we made our hypothesis. It became hard / difficult to formulate - the hypothesis, in consideration of the data we have collected. We should rather have made questions that give direct answers on our hypothesis.

³ Performance is defined as the ability to comply to a user's need.

6.1.8 Results

We can see from the result that the participants have little knowledge about the difference between the file Access systems. Possible causes can be that they don't have regular contact with the file access Control, and they are therefore not updated in this issue.

Our participants have education in computer science and due to their experience and knowledge and because of that we were expected higher score of having knowledge of file access systems. But the results from research questions revealed differently.

The reason can be that ACL's are mainly used on Windows operative systems which originally were designed as a single-user operating system that has no need for an Access control mechanism. It was invented before XP came (different users may have diversified users accounts and private files) and ACL was also implemented through various versions of UNIX (such as Solaris), are not very well known because it is not standardized, which means that different file system designs use ACL that introduces new attributes with special qualities. This makes ACL a difficult concept for the users with little experience to understand it. There were many participants that had no experience at all with ACL while many users have sufficient knowledge of UNIX permissions this because they have learned during their studies. Perhaps this is the reason why many participants felt more comfortable with the questions concerning the UNIX – permissions. We also made enquiry whether there were any companies or schools that teach Windows ACL just to see if we could get some information and how that information could differ from this, but we could not find such.

It is also very interesting to note that more men than women were choosing UNIX. UNIX seems more technical complicated compared with Windows, because many UNIX users are using Shell prompt. We can then not avoid reflecting on the question whether women are less interested in technical issues than men even if they have equal knowledge about the issues and are using computers as much as men. The different sexes might in many situations have different needs; a woman may only feel the need of a writing program and thinks that Windows is enough for that purpose, while many men often shows their interest in which technology is faster and more advanced and gives opportunity for running more demanding programmes.

This discussion leads us to the issue of gender and technology. In the late years it has been a lot of research and discussion done [37] concerning the different influences technology can have on different gender and adjustment of their needs. Often we see that the products made for men are advertised with the focus on technical solutions for instance a computer with high processor, while in promoting a computer for women, the emphasizes is more often on other factors like the external appearance.

Another explanation can be that UNIX is somehow made for men and thus has it is own environment where women are not included in the same way. But because of the low participation of women in our study more research it is worth to do more research about this issue to verify our findings in different setting.

Most participants seem to be insecure about file security. It is also quite visible that most of them have little experience concerning about file access control. It may be caused by a lack of knowledge about it or the fact that many feel they do not need protecting their files and

catalogues. The last means that if they lack the knowledge, then they may not understand the importance of the needs of file protection and security.

However, users who are not aware of the consequences of protecting their files and computer systems are threat to system security.

6.1.9 What could be done differently?

I am summarizing here what we mean could have been done differently during the research:

- We could undertake a pilot test before we formulated our research questions
- The questionnaire should have been validated
- The selection of participants should be randomly selected in order to increase the participation of women in the study.
- We should recruit participants from others places such as University of Oslo.

The ultimate goal of a study like this would be to find a way of determining an optimal solution to file access control. We would like to try a method such as that in [38], where game theory is used to find a “best balance” between competing factors, the values in the matrix represent “pay off” in our case “Quality of System (Qof)”. See the example from ref. [38] in fig. 6.1.10a for comparison. There one evaluates strategies for upgrading software in the presence of different faults.

The factors in this study are as bellowing figure 6.1.10b showing. However, we are not able to evaluate the date in this form due to the limitations of the study.

	Security holes	Bug in function	Missing function
Upgrade version now	(10,5)	(10,0)	(5,-5)
Test, then upgrade	(5,5)	(3,9)	(0,8)
Keep parallel version	(-10,5)	(-1,10)	(0,10)

Figure: 6.1.10a

System				
users	Windows ACL	Unix permissions	Ownership	groups
Ignorance	(?)	(?)	(?)	(?)
Accidental Carelessness	(?)	(?)	(?)	(?)
Intentional carelessness	(?)	(?)	(?)	(?)

Figure: 6.1.10b

The vector (n, m) describes the combination of a user's knowledge level n , and the systems inbuilt ability to respond correctly for a certain user knowledge level ($m=f(n)$)

6.2 Discussion Summary

- We have evaluated the two systems due to user experience but we have also taken into consideration the technical part of the two systems.
- The knowledge of participants on WACL is low comparing to UP despite of using WACL mostly.
- UNIX is obligatory subject at the Department of Engineering but ACL is not a part of the curriculum in this Department therefore is the knowledge of participants on WACL low.
- We find certain security weaknesses in the system caused by users.

Chapter 7

Conclusion and Recommendations

Because of the complexities of the issue and the limitations of the study, it is hard to draw a strong conclusion. Both systems clearly have both strengths and weaknesses.

There is a difference between UP and WACL File Access Systems. Many users have experienced that UNIX file access system is easier to understand since it attains three categories; the user, the group and all others.

The WACL file access system used on Windows (which originally was designed as single-user Operating system) is almost unknown for the users. While other file-systems- designs which implemented ACL's introduce their own new attributes. This makes ACL difficult for ordinary users to understand. Even if many have tried to make a simple version of ACL which is better than UP, they have not yet been able to standardize the system [33].

There is an obvious interest amongst most users to protect their files, and it is likely important for them to find ways to safeguard their documents. We find out that many users using the default value set by the system administrator, it is therefore important that they find a sufficient default value, so the user files are satisfactorily protected even if the users themselves are not aware of how the protection system works. Another important point is that the participants showed a lack of knowledge about the file access systems generally. Which means that the system users do not properly understand issue; therefore the system administrators have a big challenge in front.

The participants were categorised by *gender*, *age* and *computer- experience*, to find out which group are aware system security. We observed that youngsters' participants are more conscious about system security than the oldest participants. Women are more concerned with the *easy to use and understandable systems*, while men often show more interest in advanced and more *complicated systems and tools*.

Both systems (UP, WACL) have stronger and weaker sides, and we feel that we have got more knowledge about the participants, their habits and their skills about file systems. We can now see easier what they need to work on.

Further work: it would be nice to repeat this study in order to test the hypotheses and the formal model in section 5.2.

Appendix A

Result of Study I

Preference Group 1			
1 preference of Operating system <i>What operating system do you use?</i>	Unix	Widows	Both
	16%	70%	13%
2. deferens file access systems <i>Are there a big different between UNIX Permissions and Windows ACL's file access systems?</i>	Yes	No	Don't know
	32 %	21 %	47 %
3. Change file permissions <i>Which system do think is easiest when changing file permissions?</i>	Unix	Windows	Don,t know
	48%	17%	31 %
Usefulness Group 2			
4. Users activity on the system <i>Do open more then 5 files daily?</i>	Yes	No	
	95 %	5 %	
5. Users activity on the system <i>Do you save more then 5 files daily?</i>	Yes	No	Don't know
	67 %	32 %	2%
6. Users work place <i>What do you prefer work from home or at the school?</i>	School	Home	Both
	46 %	40 %	14 %
7. How do you save electronic documents then? <i>How do you save electronic documents then?</i>	At school	Removable + hard- disc	Not answer
	36 %	20 %	44 %
8. Do give your folders and files meaningful names <i>Do give meaningful name when saving your files?</i>	Yes	No	Don,t know
	91 %	9 %	0 %
Knowledge Group 3			
9.Users Knowledge about file systems <i>Do you know the differences between Unix and Windows file Access rights?</i>	Yes	No	Don,t know
	52 %	46 %	2 %
10.sers Knowledge about ACL's <i>Do you know what ACL is at all?</i>	Yes	No	Don,t know
	59 %	37 %	4 %
11. Users Knowledge about ACL's <i>Do you how ACL works/ function?</i>	Yes	No	
	27 %	40 %	
File right management knowledge Group 4			
12. Specify file access rights <i>Did you needed to change or specify file rigths with out succeed?</i>	Yes	No	Dont know
	83 %	16 %	1 %
13 Users Knowledge on file access rights	Yes	No	

	79 %	21 %	
<i>Do you know how to change file rights?</i>	79 %	21 %	
14. Usersfulness <i>Do think it is important to change file access rights?</i>	Yes 76 %	No 22 %	Not answer 2 %
15. Default files rights. <i>Do you change file rights or you just use default file rights in the system?</i>	Yes 76 %	No 22%	Don't know 2 %
Security Group 5			
16. Security issue <i>Have you thought that the others can copy your documents?</i>	Yes 76 %	No 22%	Don't know 2 %
17. Security issue <i>Did you know that you can password protect your files?</i>	Yes 92 %	No 5 %	Don't know 3 %
18. Security issue <i>Do take break while log on the system?</i>	Yes 92 %	No 5 %	
19. Other system users <i>Would like to recommend others users to change their file rights?</i>	Yes 49%	No 47%	Don't know 4%
20. Stop access files <i>Why do you change file access at all?</i>	To stop see the file content 10 %	To stop modify the file content 3 %	To stop both of it 38 %
It 45 % did not answer the question			
21. It is users' task to maintain his files security? <i>Do you change file permissions often?</i>	Yes 50 %	No 48 %	Do not know 2 %
22. Top secret <i>do have a documents that you do not want others to see?</i>	Yes 80 %	No 19 %	Do not know 1 %
23. How do you organized when saving data? <i>Do you save catalogues under each other?</i>	Yes 91%	No 9 %	Do not know 0 %
24. How do you organized when saving data? <i>Do you save catalogues under each other?</i>			

Appendix B

Questionnaire from Study I

En master student ved IU skal i sin hovedprosjekt gjennomføre spørreundersøkelse som går ut på sikkerhet og filsystemer (filrettighet).

Kjønn(menn/kvinne)

sett m eller k i boksen

Alder(antall år)

Rolle(student/ansatt/lærer)

sett første S,A el. L i boksen

Erfaring med data (antall år)

Sted(bedrift/skole)

sett B el.S i boksen

Bruker du Unix eller Windows operativ system?

Ja

Nei

.....

Har du lageret flere enn 5 filer i dag?

Ja

Nei

.....

Har du åpnet flere enn 5 filer i dag?

Ja

Nei

.....
.....

Lagrer du mange kataloger under hverandre ?

Ja **Nei**

.....
.....

Gir du katalogene/filene dine lesbare/meningsfylte navn?

Ja **Nei**

.....
.....

Arbeider du oftest hjemme eller på arbeidsplassen/skolen?

Ja **Nei**

.....
.....

Har du noe ganger vært borte eller tatt pause mens du er pålogget i systemet?

Aldri **Av og til** **Ofte**

.....
.....

Er du medlem i mange grupper (med delte filrettigheter)?

Ja **Nei**

.....
.....

Har du hatt behov for å spesifisere filrettigheter, uten å klare dette?

Ja **Nei**

.....
.....

Lagrer du sensitive dokumenter (privat/arbeids/skole relatert) på elektronisk medier?

Aldri **Av og til** **vanligvis**

.....
.....

Hvordan lagrer du sensitive konfidensiell informasjon

harddisk **Fellesområdet** **flyttbar disk**

.....
.....

Har du tenkt over om andre har mulighet til å kopiere dine dokumenter uten at du vet?

Ja **Nei**

.....
.....

Hvis noen har kopiert dokumentene, vil det være til skade for deg eller bedriften?

Ja

Nei

.....
.....

Vet du at du kunne beskytte katalogene eller filene dine som inneholder dokumenter som er viktig for deg med passord?

Ja

Nei

.....
.....

Har du kjennskap til hvordan du gir filrettigheter andre ?

Ja

Nei

.....
.....

Pleier du å forandre filrettighetene på file dine på ditt område?

Ja

Nei

.....
.....

Hvis ja hvorfor gjør du det?

For å hindre andre innsyn hindre modifisering Begge deler

.....
.....

Bruker default /standard rettigheter som blir forslått for deg ved oppretting av fil/katalog?

Ja Nei

.....
.....

Vet du hva ACLs (Access Control Listes) er?

Ja Nei

.....
.....

Hvis ja vet du hvordan det ACLs fungerer?

Ja Nei

.....
.....

Er det stor forskjell mellom WACL og Unix Permissions?

Ja Nei

.....
.....

Vet du hva som er forskjell mellom rettighetene i Unix filsystemer og Windows filsystemer?

Ja Nei

.....
.....

Hvilken av de to file- systemene som er nevnte ovenfor synes du er lettest sette/endre fil/katalog rettigheter på?

Ja **Nei**

.....
.....

Har du nytte av å endre filrettighetene?

Ja **Nei**

.....
.....

Ville du råde alle som bruker nettverkssystemet til å bruke endre default filrettighetene?

Ja **Nei**

.....
.....

Hva ville du endre hvis det er noe du ikke liker?

Ja **Nei**

.....

Appendix C

Results from study II

Knowledge of file rights

1. Do you think it is ok to set rights 777 when delegating file rights to your friend?	Correct answer	Wrong answer	Did know
	24	1	3
2. If 'no', what access rights would you give to your friend?	Correct answer	Wrong	Did know
3. What is the default right, when a new group member is defined?	Correct answer	Wrong answer	Did know
	3	14	11
4. What does the command 'umask' do?	Correct answer	Wrong answer	Did know
5. Can you differ between catalogues and files with the command 'chmod -r'?	Correct answer	Wrong answer	Did know
	6	10	11
6. Does write-access automatically imply read-access?	3	7	9
7. What does this mean: rwx rw- r--?	Correct answer	Wrong answer	Did know
8. How do you set file or catalogue-rights in Windows?	15	1	4
9. What command do you use when you want to list files og catalogues in DOS-command window?	Correct answer	Wrong answer	Did know
10. Is there another, easier way to change rights in Windows?	12	4	11
11. What command do you use when you set rights in Novell Netware?	Correct answer	Wrong answer	Did know
	1	1	15
12. What command do you use when you set rights in Novell Windows 2000/XP?	Correct answer	Wrong answer	Did know
	0	2	25
13. What command do you use to set rights in Unix?	Correct answer	Wrong answer	Did know
	0	0	27
14. What command do you use when you are setting rights in Linux?	Correct answer	Wrong answer	Did know
	19	3	5

The questions from study II will be showing here while the Results will not showing any where. Because most of partcipents answer "I dont know " the rults of those who answer correct, was used as a supplemt in study 1. We just showing here how many of those asked have answered wrong and how many have answered right.

Appendix D

Questionnaire from Study II

Spørreundersøkelse 2

Windows ACL OG Unix file permisjons test til studentene og ansatte på UI.

Tror du det er passende å sette rettigheter til 777 for å gi file rettighet til din kamerat?

.....

Hvis nei, hva slags rettigheter ville du satt da?

.....

Hva er default rettigheter som operates for en gruppe medlem?

.....

Hva gjør kommandoen Umask?

.....

Kan du skille mellom kataloger og filer med kommandoen "chmod -r"

.....

Gir skriverettigheter automatisk leserettigheter?

.....

Hva betyr dette: rwx rw- r--?

.....

Hvordan setter du file eller katalog rettigheter på Windows?

.....

Hvilken kommando bruker du når du skal liste opp filer eller kataloger på DOS vindu på Windows?

.....

Finnes det en annen måte som er enklere å endre katalogrettighetene på Windows? Hvordan?

.....

Hvilken kommando bruker du når du setter rettigheter på Novell net ware?

.....

Hvilken kommando bruker du når du setter rettigheter på Windows 2000/XP?

.....

Hvilken kommando bruker du når du setter rettigheter på Windows Unix/ Solaris?

.....

Takk for at du tok dag tid til å delta i vår prosjekt undersøkelse

Appendix E

Questionnaire from Study II

Intervju tatt fra to system ansvarlig på Ingeniør høgskolen.

Svare fra den delen blir ikke vist på noe sted. Fordi mening var ikke å analysere disse, men å få lit ekstra informasjon fra noen som kan bra om begge systemene.

1. Hvor gammel er du?

.....
.....

2. Hvor lenge har du jobbet med data?

.....
.....

3. Hva er din stilling/status?

.....
.....

4. Kan du fortelle lit om det du jobber med til daglig?

.....
.....

5. Hva vil det si at et system er lett å administrere?

.....
.....

6. Etter din mening og erfaring, hvilken av følgende systemer synes du er let å administrer?

.....
.....

7. Hva er største forskjellen på de to systemene?

.....
.....

8. Hvilken av de synes du er let å bruke, fra en bruker stå sted?

.....
.....

Appendix F

Glossary

authenticity	the aspect of security that recognizes a person in association with a certain role
catalogue	groupings of files
entity	any subject, such as persons, services, processes, programs
file	data stored in a computer
file access control	protection of files
manageability	the aspect of security that delegates roles to entities according to level of user knowledge
operating system	the primary software controlling the behaviour of the hardware
privacy	the aspect of security that governs ownership to dataobjects

Appendix G

Progress Schedule

FREMDRIFTSPLAN

Project: Evaluation of File Access Control Implementations

Uke	1-4	4-8	9-13	14-20	21 og utover
Dato	2005.01.24 - 2005.01.30	2005.01.30 - 2005.02.27	2005.02.28 - 2005.03.03	2005.03.04 - 2005.05.22	2005.05.23 - ...
Gjøremål	Samtaler med veilederen	Systematisere innsamlet materiale	Analysere spørreundersøkelsen	Samråd med veileder	Forberede muntlig presentasjon
	Definere mål og utarbeide plan	Skrive om bakgrunn og historikk	Statistisk vurdering	Skriftlig formulering	
	Få godkjenning av plan	Undersøke ACL&UnixPerm 'first-hand'	Fullføre matrise	Leverer utkast til konklusjon til veileder	
	Samle stoff	Utarbeide/innhente spørreundersøkelse	Vurdering av resultat	Korrektur basert på feedback	
	Litteratur lesning og notater	Påstarte sikkerhetsstrategi-matrisen	Trekke konklusjon		

fase 1	Problemdefinisjon
fase 2	Informasjonshenting
fase 3	Analyse
fase 4	Konklusjon
fase 5	Presentasjon

References

1. Axel van Lamsweerde. Elaborating Security Requirements by Construction of Intentional Anti- Models. *Proceedings of the 26th International Conference on Software Engineering*, May 2004
2. Bishop Matt. Computer Security Art and Science, *Addison –Wesley*, 2003
3. Rouse W.B. A Human –Cantered Approach to Designing successfull products and Systems. Wiley series in Systems Engineering, Vol 2, Wiely & Sons 1991
3. Generic Virtual Memory Management for Operating System Kernels E. Abrossimov, M. Rozier, M. Shapiro 2000
4. Rasmussen J. Information Processing and Human –Machine Interaction and Approach to Cognitive Engineering, North-Holland serier in System Sceince and Engineering Vol 12, New York: North-Holland 1996.
5. Shneiderman B. Designing the User Interface Strategies for Effective Human –Computer Interaction, Addison Wesley Publishing Company 1986, isbn 0-201-16505-8
7. Rasmussen .J Information Processing and Human- Machine Interaction Engineering vol. 12, New York North –Holland, 1986
8. McRues D. Human Dynamics in Man-Machine Systems *Automatica*, vol 16, pp.237-253. 1980.
9. Endsley M. R. Towards a theory of Situation Awareness in Dynamics Systems, *Human Factors* pp.32-64.1995.
9. Jeff Sedayao, Cisco IOS Access List O,Reilly 2001.
10. Jung-Min Kang, Wook Shin, C-G. Park, Dong-Ik Lee. Extended BLP Security Model Based on Process Reliability for Secure Linux Kernel. December 2001, *Proceedings of the 2001 Pacific Rim International Symposium on Dependable Computing*
11. Walcott Tom, Bishop Matt. Traducement: A Model for Record Security November 2004, *ACM Transactions on Information and System Security (TISSEC)*, Volume 7 Issue 4
12. Carl E. Landwehr, Constance L. Heitmeyer, John McLean A Security Model for Military Message Systems. August 1984. *ACM Transactions on Computer Systems (TOCS)*, Volume 2 Issue 3
12. Udo Halfmann, Winfried E. Kühnhauser. Embedding Security Policies into a Distributed Computing-Environment. April 1999, *ACM SIGOPS Operating Systems Review*, Volume 33 Issue 2.
13. Vijayalakshmi Atluri, Soon Ae Chun, Pietro Mazzoleni. Access Control; Chinese wall; security model for decentralized workflow systems. November 2001, *Proceedings of the 8th ACM conference on Computer and Communications Security*
13. Dr. David F.C. Brewer and Dr. Michael J. Nash
The Chinese Wall Security Policy1. Published at the IEEE Symposium on Research in Security and Privacy 1-3, May 1989, Oakland, California (pp. 206-214) © 1989 IEEE.
14. J. Mclean Reasoning. About Security Models, in proceedings of the 1987 IEEE Symposium on security and privacy
15. Irene Hu. Measuring file access patterns in UNIX August 1986, *ACM SIGMETRICS Performance Evaluation Review*, Volume 14 Issue 2

15. Greg Lehey Features. Closed Source Fights Back, July 2003, Queue, Volume 1 Issue 5
16. Charles Severance
http://vertigo.hsrl.rutgers.edu/ug/unix_history.html
18. Jerome H. Saltzer. Protection and the control of information sharing in multics
July 1974. Communications of the ACM, Volume 17 Issue 7
18. <http://www.theiia.org/itaudit/index.cfm?fuseaction=forum&fid=53>
Automation Magazine - Cork Publishing Ltd, United Kingdom, Vol. 1, November 1998.
18. <http://www.theiia.org/itaudit/index.cfm?fuseaction=forum&fid=53>
Automation Magazine - Cork Publishing Ltd, United Kingdom, Vol. 1, November 1998.
19. G. UNTER KARJOTH. Access control with IBM Tivoli access manager
ACM Transactions on Information and System Security (TISSEC) Volume 6,
Issue 2 May 2003.
20. B. LAMPART. Protection ACM Operating System, Reviews 1974.
21. <http://docs.hp.com/en/B8725-90053/ch03s02.html>
22. Dieter Gollmann. Computer Security. John Wiley & Sons 1999.
22. Johns Quarterman, Abraham Silberschatz, and James L. Peterson
4.2BSD and 4.3BSD as Examples of the UNIX System, December 1985, ACM Computing Surveys (CSUR),
Volume 17 Issue 4
23. Michael M. Swift, Anne Hopkins, Peter Brundrett, Cliff Van Dyke, Praerit Garg, Shannon Chan, Mario
Goertzel, Gregory Jensen. Improving the granularity of access control for Windows 2000. November 2002, ACM
Transactions on Information and System Security (TISSEC), Volume 5 Issue 4
24. Gilbert Hel. Working with Cisco Access Lists May 1999, International Journal of Network
Management, Volume 9 Issue 3
25. Basic Windows File Permissions (ACLs)
<http://www.le.ac.uk/cc/dsss/docs/acls1.shtml#int>
25. Burgess M. Principles of Network and Network and System Administration, John Wiley & Sons 2004
27. Fergus D. and David. J. Han. Elements of Statistics, Addison Wesley 1995
28. Gunnar G. Løvå. Statistikk 1999.
32. Andreas Cgrunbacher. POSIX Access Control Lists on Linux, Publication at the USENIX Annual Technical
Conference, San Antonio Texas, June 2003
33. Davis, R and Alla H. Petri Nets. Modelling of Dynamic Systems- A Survey, Automatica, vol 30, No 2, 1994.
34. Chalmers, B. A, Burns C.M and Bryant, D. J. Domain Modelling, June 2001
35. Rouse, W. B. Hammer, J.M and Lewis, C. Capturing Human Skills and knowledge.
IEEE, Transactions on Systems, Man and Cybernetics, Vol SMC-19. No 3. May/June 1989

36. Rasmussen J. Skills, Rules and Knowledge; Signals, Signs, and Symbols and Human Performance Models, IEEE, Transactions on System, Man and Cybernetics, Vol SMC-13. No 3. May/June 1983.

37. Lie M. He, She and IT Revisited New perspectives on Gender in the Information Society
Gyldendal norsk forlag 2003

38. Burgess M. Analytical Network and System Administration.
Managing Human- Computer System, John Wiley & Sons, 2004