Modernising MAC: New Forms for Mandatory Access Control in an Era of DRM

William J Caelli
1 Information Security Institute, Queensland University of Technology,
GPO Box 2434, Brisbane. Queensland. 4001. Australia.
w.caelli@qut.edu.au
and
International Information Security Consultants Pty Ltd,
21 Castle Hill Drive South, Gaven. Queensland. 4211. Australia.
w.caelli@iisec.com.au

Abstract. By its definition "discretionary access control" or "DAC" was not designed or intended for use in the untrusted environment of current globally connected information systems. In addition, DAC assumed control and responsibility for all programs vested in the user; a situation now largely obsolete with the rapid development of the software industry itself. However, the superior "mandatory access control" or "MAC" specifications and resulting implementations proved to be unacceptable for commercially oriented systems and their managers. For example, the USA's National Security Agency's (NSA) "Secure LINUX" or *"SELinux",* program made available under open source arrangements in 2000, aims at changing this state so that the benefits of MAC technology could be used to "harden" commodity ICT products. This paper analyses the need to abandon DAC, suggests variations and enhancements to basic access control concepts and relates the technology to the particular requirements of the "home computer". However, the potential for this technology to be used to limit competition must also be considered as a new participant is considered, i.e. the "owner" of software or allied systems wishing to impose digital rights management (DRM) requirements on the legitimate user.

1 Introduction

The microcomputer revolution [1] not only introduced the world to the commoditization of the computer hardware industry but it also heralded the rapid and accelerating growth of the overall software industry including, most notably, the "packaged software" sector. From the earliest days of use of computer systems for business and commerce applications, such as the LEO system of the mid-1950s, commercial software systems had been largely developed, tested, deployed and managed by "in-house" systems analysis and software development teams. Indeed, as large time-sharing/batch processing operating systems came into commercial usage in the early 1960s, e.g. the IBM System/360's OS/360 system, the realization that information security was becoming a concern started to arise. The USA's "Ware Report" of 1970 [2] illustrates this trend most notably. By the early 1970s computer usage had started to outgrow the physical security boundaries of the well established "computer" or "data processing" centre of the previous 20 years. Timesharing introduced the "end-user" to computer systems, e.g. firstly the creation of the FORTRAN programming language, largely used in batch processing form at the time, and then the development of the BASIC programming language for use by scientists and engineers to create their own software systems in an on-line, real-time, terminal oriented environment. In this emerging situation, it became essential that users could be protected from each other and the basic operating system and allied library structures of the main system protected from all users. The MULTICS project of the late 1960s and on till the 1980s emphasized the development of protection/security architectures and structures to achieve these goals.

In 1985, IBM sent out a *"security questionnaire"* which set out a number of pertinent questions. These included:

"21. Do operating systems provide adequate user-to-user isolation for the intended applications and environments ?

Are they able to protect themselves from disorderly behaviour by users ?

22. Are applications free from outside interference ?

23. Is data free from outside contamination ?

24. Are authorized changes to the operating systems controlled to maintain the ability to protect themselves from users ?

..... etc. "

The questions pointed to growing concern about the very security environment that was emerging by that time as commodity personal computer systems started to have an influence on the IT marketplace and such systems had started to be adopted for mission critical commercial level applications. Interestingly, this questionnaire is from the same year as the release of the final version of the USA's "Trusted Computer Systems Evaluation Criteria (TCSEC)", i.e. the *"Orange Book"*. This famous document had three major aims that are equally applicable today, as follows:

"(a) to provide users with a yardstick with which to assess the degree of trust that can be placed in computer systems for the secure processing of classified or other sensitive information;

(b) to provide guidance to manufacturers as to what to build into their new, widely-available trusted commercial products in order to satisfy trust requirements for sensitive applications; and
(c) to provide a basis for specifying security requirements in acquisition specifications."
From the outset it can be seen that a clear commercial emphasis is placed on the creation and propagation of such security parameters.

However, even by 1994 the impression, and indeed the reality, of a decline in computer systems security from the 1970s was widespread despite the existence of the "orange Book" and its allied documents that formed the so-called "Rainbow Series" of specifications. By this time the microcomputer/PC revolution dominated the ICT industry and Internet based global connectivity of these untrusted systems emerged. The feeling was summed up by Kay [3] in 1994 as follows:

"… Security is an issue because the majority of today's operating systems – both stand alone and networked – were developed without any consideration for security capability whatsoever, or security and control features were tacked on as an afterthought…"

1.1 Access Control

Corbato [4] clearly set out a major parameter for what was to become known as time-sharing operations on a central computer in a 1965 paper on the MULTICS system with the following requirements statement:

"Finally, as noted earlier, the value of a timesharing system lies not only in providing, in effect, a ***private computer*** *to a number of people simultaneously, but, above all, in the services that the system places at the fingertips of the users."*

(The emphasis is from this author.) This system became operational and in use at M.I.T. by 1969 and was later commercialized. Now, this concept of user separation, in essence a private (personal) computer, is fundamental to all forms of "trusted" usage in computer systems and forms the base of what has become known as the lowest form of control for a computer system, i.e. *"discretionary access control (DAC)"*. However, there are very severe limits to this paradigm as the Orange Book explained.

Therefore, before continuing it is worthwhile to consider the overall and general requirements that were set by the Orange Book as bases for any secure system. These were as follows, in abridged form:

"Fundamental Computer Security Requirements
Any discussion of computer security necessarily starts from a statement of requirements, i.e., what it really means to call a computer system "secure." In general, secure systems will control, through use of specific security features, access to information such that only properly authorized individuals, or processes operating on their behalf, will have access to read, write, create, or delete information. Six fundamental requirements are derived from this basic statement of objective…

Policy

Requirement 1 - SECURITY POLICY - There must be an explicit and well-defined security policy enforced by the system……
Requirement 2 - MARKING - Access control labels must be associated with objects….

Accountability

Requirement 3 - IDENTIFICATION - Individual subjects must be identified …
Requirement 4 - ACCOUNTABILITY - Audit information must be selectively kept and protected so that actions affecting security can be traced to the responsible party……

Assurance

Requirement 5 - ASSURANCE - The computer system must contain hardware/software mechanisms that can be independently evaluated to provide sufficient assurance that the system enforces requirements 1 through 4 above….
Requirement 6 - CONTINUOUS PROTECTION - The trusted mechanisms that enforce these basic requirements must be continuously protected against tampering and/or unauthorized changes….. "

The Orange Book went on to define some four hierarchical "divisions", viz. D, C, B and A, with divisions C and B being further divided up into "classes", viz. C1, C2, B1, B2, B3. Division A was the "highest" security specification and D the lowest or "minimal" division. Today, almost all commercial operating systems lie in the "C1/C2" class providing *"discretionary access control"*. These provide simply *"separation of users and data."* Moreover, these classes are intended to have *"some form of credible controls capable of enforcing access limitations on an individual basis, i.e., ostensibly suitable for allowing users to be able to protect project or private information and to keep other users from accidentally reading or destroying their data."* However, and most importantly, the operating "environment" for these "C1/C2" systems is *"expected to be one of cooperating users processing data at the same level(s) of sensitivity."* In the age of global interconnection of host servers and client systems via the Internet, with unknown and even hostile users in existence willing to attack other systems, the concept of "cooperating users" is no longer relevant and these classes of systems should have long ago been clearly seen as unsafe and obsolete in the new interconnected environment. However, this is clearly not the case.

Moving to a higher, more secure division, the "B" or "mandatory access control (MAC)" division the parameters suddenly change. Starting at Class B1 the following applies:

"Class (B1) systems require all the features required for class (C2). In addition, an informal statement of the security policy model, data labelling, and mandatory access control over named subjects and objects must be present. The capability must exist for accurately labelling exported information."

At last some form of acknowledgement of the needs for connected security comes to the fore. By Class B2, the Class that seems to most reliably represent the situation in 2007, the security features of a modern operating systems and allied components

can be clearly seen. Indeed the Orange Book itself contrasted discretionary access control (DAC) and mandatory access control (MAC) as follows:

"Discretionary security is the principal type of access control available in computer systems today. The basis of this kind of security is that an individual user, or program operating on his behalf, is allowed to specify explicitly the types of access other users may have to information under his control. Discretionary security differs from mandatory security in that it implements an access control policy on the basis of an individual's need-to-know as opposed to mandatory controls which are driven by the classification or sensitivity designation of the information. Discretionary controls are not a replacement for mandatory controls."

Even later attempts by the USA to force, or at least influence, its Department of Defence to enter into purchase of systems designed and evaluated around the Orange Book's "C2" specification achieved little, as Ryan [5] points out as follows:

"The Computer Security Act of 1987 was interpreted into policy by the DoD as requiring all computer systems to be C2-compliant by 1992, a policy known as 'C2 by '92.' "

There was also discussion at the time of making an even higher bid for computer security in the USA's Department of Defense with another, unheeded call for *"B2 by '95"* to surpass that 1992 deadline. In summary, the basic admonition of the Orange Book never really came to reality, i.e. *"to encourage the Computer Industry to develop trusted computer systems and products, making them widely available in the commercial market place. Achievement of this goal will require recognition and articulation by both the public and private sectors of a need and demand for such products."*

2 Rethinking MAC

2.1 Problem Description

In simple terms, the requirements at the enterprise level for efficient and effective access control can be paraphrased from the 4th of the USA's Computing Research Association's (CRA) *"Grand Challenges"* in computer and information security [6] set out in 2003. The 4th challenge stated as follows, and can be regarded as still being significant today:

"Give end-users security controls they can understand and privacy they can control for the dynamic, pervasive computing environments of the future."

From an enterprise perspective a "new MAC" paradigm could be proposed based on the CRA challenge above, as follows;

"Give the CIO security controls they can understand and enforcement they can control for the dynamic, pervasive computing environments of the future."

At the same time Microsoft has introduced a next generation of operating system, Windows Vista, that, according to BusinessWeek [7]*"shakes up the ecosystem"*. In particular the BusinessWeek article cited above clearly identifies the "hardening" of security in the system as a major factor; a factor of particular note to producers of commodity product level software to operate on this platform. The article presents the challenge to these companies in the following way;

"Vista also introduces big changes in the way programs install files on a PC's hard drive, log users in, and handle security functions. That could cost software companies lots of engineering time and support calls—and sap profits, says Simon Heap, a partner at consultancy Bain & Co., which advises makers of business software."

Some new and important factors have now arisen. The rapid rise of the software industry also led to questions of "software piracy" and the legitimate usage of purchased packaged systems. This meant that a new "user", so to speak, now entered the computer system; one whose interests were allied to "digital rights management (DRM)", i.e. the enforcement of whatever terms and conditions of use had been placed on the software in use, and whose "enemy" may actually be the "customer" who had purchased a license to use the software. Indeed, this development is not considered at all in the earlier "Orange Book" case where, it would appear, the model in use is one where all software systems, particularly application systems, have been designed, developed, tested and installed by the "owner" of the system who now also manages the operation of these systems.

Many enterprises no longer maintain any internal ICT professional group in the sense that such a group is chartered with the design and development of application or sub-system software for use by the enterprise. Software is now a purchased commodity, installed and operated by end-users in most cases.

2.2 The Trouble with DAC.

Figure 1 : Microsoft Inc "XENIX" system – 1984. (Source: Wikipedia – Feb 2007)

Into the 1990s attempts were made to make "B-level" trusted systems with MAC capability commercial realities. An example is *"Trusted XENIX",* a special version from "Trusted Information Systems Inc." of Microsoft's "XENIX" operating system developed for the Intel x86 CPU chip set from an AT&T UNIX licence in the late 1970s. Other activities included research projects aimed at a similar level of trusted system behaviour. These included the "Trusted MACH (TMach)" project aimed at a high trust version of the Mach micro-kernel system. In addition the "SEVMS", by

Digital Equipment Corporation [8] implemented *"..a mandatory (i.e. non-discretionary) access control mechanism"* with the claimed property that it *"..is an implementation of a security policy which is beyond direct user control. This security policy is centrally and uniformly established by the system security manager (often the system manager). SEVMS is responsible for enforcing the security policy established by the security manager."* Similarly "Trusted Solaris" [9] from SUN Microsystems aimed at the same philosophy. This is summarized in the Trusted Solaris data sheet as follows:

"MAC hierarchical and compartmentalized labels correspond to the sensitivity of information that must be kept separate, even when it is stored on a single system. Because information labeling happens automatically, MAC is mandatory. Ordinary users cannot change labels unless the system administrator gives them special authorization. In fact, users with labels in separate compartments are not allowed to share information. By enhancing and extending security mechanisms, Trusted Solaris 8 software provides additional protection for servers and desktop systems that process highly sensitive information."

2.3 Themes and Challenges

The past thirty years or more has seen a number of security models developed, meeting complementary requirements for security in computer systems. [10, 11] Experimental and "small run" operating systems have been developed and deployed using these models but none, outside the basic "access control list (ACL)" structure has really been accepted in mass market operating systems and allied software products.

Thus, the challenge of "modernizing MAC" can best be considered in the light of four distinct themes or broad categorizations of information systems usage. These are:

a. Large enterprises, both public and private,
b. Small to medium enterprises,
c. Micro-businesses, and
d. Individual or home users.

Within each of these broad categories a number of challenges can be set out, as follows.

2.3.1 Large Enterprises, Public and Private

The challenges here are mainly personnel based. These may be summarized as follows:

- comprehensibility to the normal enterprise CIO,
- mapping of commercial enterprise parameters and risk assessment processes to a new paradigm,
- incorporating risk assessment and management processes into the mandatory-style regime,

- development of assessment methods for the system definition and procurement stages,
- appropriate "profile" definition and management packages aligned to enterprise realities and integrated into enterprise level systems,
- appropriate education and training for the CIO,
- education and training for application system developers, and
- appropriate cost evaluation parameters for senior management, including any necessary retraining and allied expenses.

2.3.2 Small to Medium Enterprise

In this case it must be assumed that some ICT professional resources are available to the enterprise, either "in-house" or by contract. The challenges become a sub-set of the ones above:

- availability of appropriate security/profiling definition tools mapped to medium enterprise needs,
- incorporation of MAC "awareness" into packaged systems relevant to this class of enterprise, and
- higher levels of education and training tools.

2.3.3 Micro-enterprises

This category of enterprise covers the normal "small-office, home-office (SOHO)" category of enterprise consisting of under 10 staff members, for example. This business profile means that the enterprise does not have any "in-house" ICT professional assistance and, as needed, will normally employ appropriate contractors in the necessary area. The challenges here are quite different and important since this class of enterprise which, once connected to the global Internet using commodity level hardware and software products, becomes a target for attack and compromise. Some challenges in this situation are:

- incorporation of MAC facilities into popular business information systems used by this class of enterprise,
- simplified schemes for the installation and management of MAC oriented operating systems and relevant software systems, and
- education and training of the application software enterprises catering to this class of user.

2.3.4 Home User

This, the largest category of user, has unique requirements. The DAC paradigm has meant that computer programs loaded into a home computer from other computer systems connected to the global Internet have largely "inherited" the access parameters of the user and software system used to load such packages, e.g. the "browser", email handler, etc. recent attempts, e.g. by Microsoft Inc of the USA with

its "Windows/Mandatory Integrity Control (W/MIC)" concept has started on path towards the need to separate the information environment of the home user from that assumed by software packages "invited" into the system. The challenges for MAC in this environment appear to include:

- transparency of the underlying MAC level complexity from the end-user/administrator,
- simplification of the labeling requirements inherent in MAC design,
- provision of understandable and easily administered "profiles" covering the normal processes undertaken on a "personal/home" computer system.

2.4 Digital Rights Management and Encryption

A string new role "player" has come to the fore in the 21st century. This is the role of the software/content "owner" whose "enemy", in a way, is its very own customer. Digital rights management (DRM) introduces in to the MAC paradigm a parameter not normally considered in the past in defining the appropriate access control models, e.g. read/write/append/delete permissions, etc. Today, DRM systems may be required to limit legitimate and authorized systems users from certain activities within their own computer systems, e.g. read from one file and write to another such as is required to "copy" data from a "source" to a "target". At present, DRM enforcement schemes at the operating systems level appear to be limited to the following incomplete list of methods and schemes,

- use of encryption/decryption processes to restrict access to data,
- control of the encryption/decryption processes themselves through restrictions on access to operating systems components, such as device drivers, etc., an example being access to the device driver sub-systems for high density DVD units,
- control of the necessary cryptographic "key" structures required by the encryption/decryption processes, and
- use of "privilege" restrictions to separate access rights of legitimate users from those which are claimed by the "owner" of the data, e.g. copyright holder, etc.

An open research question exists in relation to the most appropriate technologies required to integrate cryptographic sub-systems into MAC operating system architecture. While such systems as "SELinux" have started to address this problem with appropriate interface definitions and appropriate kernel level architectures, the high level relationships between such cryptographic sub-systems and end-user/process profiles is still largely unresolved.

3. Conclusions.

This paper has proposed that there are many challenges to the goal of making MAC security architectures relevant and useful at the commercial and commodity computer system level. These challenges are both technical and administrative. At the same time, the lack of and need for appropriate information security education

and training is seen as a barrier to the commercial acceptance of "hardened" MAC-based operating systems and allied structures.

Acknowledgments

This overall research program has been supported by a grant from the Australian Research Council (ARC).

References

1. Caelli, W., The Microcomputer Revolution: Some Social Implications of Advanced Technology, (Monograph No. 1, Australian Computer Society, Sydney, 1979. ISBN 0-909925-21-6).
2. Ware, W. H., ed., Security Controls for Computer Systems: Report of Defense Science Board Task Force on Computer Security, AD # A076617/0, Rand Corporation, Santa Monica, Calif., February 1970, reissued October 1979.
3. Kay. R., Distributed and Secure, BYTE Vol. 19, No. 6, June 1994, Pg. 165.
4. F. J. Corbato and V. A. Vyssotsky, Introduction and Overview of the Multics System, Fall Joint Computer Conference 1965; http://www.multicians.org/fjcc1.html.
5. Ryan J., The Effect of Public Budgetary and Policy Decisions on Development of Trusted Systems, http://www.gwu.edu/~asem_dc/RyanASEM02.html.
6. http://www.cra.org/Activities/grand.challenges/security/home.html.
7. http://www.businessweek.com/technology/content/feb2007/tc20070222_677788.htm?link_position=link1 Accessed at 24 Feb 2007.
8. SEVMS User's Guide, Order Number: AA-QC05A-TE, November 1994, Digital Equipment Corporation, Massachusetts. USA.
9. http://www.sun.com/software/solaris/trustedsolaris/ds-ts8/index.xml.
10. Summers, R, C., An overview of computer security, IBM Systems Journal, Vol. 23, No. 4, 1984.
11. Ames, S. R. and Neumann, P., Guest Editors' Introduction: Computer Security Technology, Computer, Vol. 16, No. 7. July 1983.