"B IS FOR BUSINESS : MANDATORY SECURITY CRITERIA AND THE OECD GUIDELINES FOR INFORMATION SYSTEMS SECURITY"

Professor William J Caelli
Head
School of Data Communications
and
Member
Information Security Research Centre (ISRC)
School of Data Communications
Faculty of Information Technology
Queensland University of Technology
GPO Box 2434
BRISBANE, QUEENSLAND, AUSTRALIA
Tel:+61-7-3864 2752
Fax:+61-7-3221 2384
Email:caelli@fit.qut.edu.au

Paper submitted to the
19th National Information Systems Security Conference,
Baltimore, MD, USA, October 22-25, 1996.

Abstract:

This paper sets out the proposition that ***mandatory*** security functionality, with its associated enforcement and evaluation criteria, are required in computer and data network systems to meet emerging national and international laws and guidelines for information systems security. The OECD 1992 Guidelines for Information Systems Security are used as a baseline for the consideration of such levels of trusted functionality. Concepts for trusted computer and data network systems, as set out in the original Trusted Computer System Evaluation Criteria (TCSEC) of the United States, the Information Technology Security Evaluation Criteria (ITSEC) of the group of four European nations, the Canadian (CTCPEC) evaluation criteria and the more recent international Common Criteria (CC) are seen as relevant to the distributed and client/server computing environments of information systems in the 1990s and beyond. Overall, it is suggested that security functionality and evaluation/ enforcement, at the level of the earlier TCSEC "B1" as a minimum, are required in networked computer systems to meet emerging national and international legal requirements and I.T. security guidelines.

Keywords:

mandatory computer security, OECD security guidelines, TCSEC, ITSEC, Orange Book.

"B IS FOR BUSINESS : MANDATORY SECURITY CRITERIA AND THE OECD GUIDELINES FOR INFORMATION SYSTEMS SECURITY"

1. Introduction - TCSEC/ITSEC AND THE OECD Security Principles, 1992

1.1 Introduction

In 1992 the Organisation for Economic Co-operation and Development, or OECD, [OECD-92] created a set of "Guidelines for the Security of Information Systems". These guidelines follow an earlier set in 1980 covering the provision of privacy in relation to stored and transmitted data [OECD-80]. Together these guideline documents have had a marked affect on the development of associated legislation and standards worldwide at the national, regional and international levels. This paper argues that in order to meet the managerial level requirements set out in these guideline documents, information technology (IT) professionals, owners and users of information systems and appointed managers of information systems must move to a "mandatory" concept of system security facilities in order to develop and operate information systems that comply with the guideline requirements.

The key theme of this paper is that **mandatory access control** , as set out in the original "Orange Book", the Trusted Computer System Evaluation Criteria or TCSEC [TCSE-83] and later computer security evaluation criteria such as the Information Technology Security Evaluation Criteria or ITSEC [ITSE-90] and the Common Criteria or CC [CC-96] represent a minimal requirement for protection in distributed computer systems linked via data networks and operating under a "client-server" paradigm for applications. This argument is made on the basis of emerging national and international legislation and guidelines covering both **privacy** and **information systems security** which place mandatory obligations on users, owners and developers of information systems to safeguard the information entrusted to them. It is argued that lower level **discretionary** security is insufficient to provide reasonable security assurances in interconnected systems, particularly where such activities as acceptance of "scripted" programs by a host computer from a remote system may be allowed. The provision of mandatory security services will also form a basis for what may be called "self-defending objects", a scheme whereby distributed object oriented systems may make intelligent security related decisions about requests made to them from remote and often unknown sites.

1.2 The OECD Guidelines

On the 26th of November 1992 the Council of the OECD adopted a document known as the:

> *"Recommendation of the Council Concerning Guidelines for the security of Information Systems".*

These were then adopted by the 24 member nations of the OECD. The document of interest here is composed of three parts, consisting of the "Recommendation" above plus:

> *"Guidelines for the Security of Information Systems"*; and
> *"Explanatory Memorandum to Accompany the Guidelines for the Security of Information Systems".*

The "Guidelines" themselves set out **nine principles** for security which are set out in Section 2. The "Recommendation" sets out the responses that member nations should have to the guidelines document. In particular it states that member countries should:

1. *establish measures, practices and procedures to reflect the principles.....*
2. *consult, co-ordinate and co-operate in the implementation of the Guidelines, including international collaboration to develop compatible standards, measures, practices and procedures .....*
3. *agree as expeditiously as possible on specific initiatives for the application of the Guidelines,*
4. *disseminate extensively the principles...*

5. *review the Guidelines every five years with a view to improving international co-operation on issues relating to the security of information systems."*

An important consideration has to be one of the response of IT professionals worldwide, through their professional organisations and through their international body, the International Federation for Information Processing (IFIP), to these Guidelines and the associated Recommendations. It is likely that legally binding parameters may emerge in the 1990s that govern the responsibilities of IT professionals, information systems owners/users and system managers alike. In this sense the underlying technology that enables security to be incorporated into information systems becomes critically important. Thus, consideration of any technical guidelines and parameters for judging such security becomes important since these, along with the Guidelines, could become "base-lines" or "codes of minimal acceptable practice" by which IT professionals, in particular, may be judged. Such judgements may even take the form of legally binding decisions through the judicial system as well as being a more general form of assessment adopted by society at large.

The actual Guidelines themselves are *"addressed to the public and private sectors"* and apply *"to all information systems"*. Moreover, the scope of the guidelines is one based around the generally accepted definition of security, i.e. the confidentiality, integrity and availability of information systems. The Guidelines also have a set of six stated "Intentions" of which one, "... to foster confidence in information systems and the manner in which they are provided and used..." is pertinent to this paper. In summary, it is submitted that such "confidence" can only really be generated in information systems, that now consist of connected host systems on national and international data networks, by incorporation of so-called "mandatory" computer security technology in the base computer systems and data networks themselves.

1.3 National and International Legislation and Guidelines

Following on from the OECD Guidelines there has been a number of initiatives at the national level, e.g. in the United Kingdom, Australia, and elsewhere, to give greater force to these guidelines in line with the recommendations of the OECD. The "Code of Practice for Information Security Management" [BSI-93] of the United Kingdom, now a British Standards Institute standard, BS-7799, sets out specific requirements that may be:

> *" .... used as a common reference standard for inter-company trading and for sub-contracting or procurement of information technology (IT) services or products."*
>
> It goes on further to state that:
>
> *" ... Information security threats are expected to become more widespread, more ambitious and increasingly more sophisticated."*

This code clearly sets out parameters that could be reasonably determined to be minimal "statements of due care" in relation to the responsibilities of IT professionals and system managers. In this sense, these codes and guidelines may start to take on some form of legal force when offered as guides in any legal proceedings.

These documents are starting to set a scene under which computer and data network security will increasingly become the responsibility of IT professionals and managers in a legally binding sense. At the same time, then, these IT professionals and managers will need to be sure that the products and systems used to create an overall enterprise wide and cross-enterprise information system are "safe to use" for such needs.

1.4 Evaluation Criteria

The USA's National Research Council [NRC-91] described security evaluation criteria in the following terms:

> *"At a minimum, security evaluation criteria provide a standard language for expressing security characteristics and establish an objective basis for evaluating a product relative to these characteristics..."*

This clearly identifies security evaluation criteria as relevant when considering the OECD guidelines.

The earliest attempts at creating such documents belongs essentially to the United States Department of Defense [TCSE-83] and the resulting "Trusted Computer System Evaluation Criteria" or TCSEC. Work had started in the late 1970s under both the United States Department of Defense (DoD) and the National Bureau of Standards (NBS), with the assistance of the Mitre Corporation, to create base documents that addressed computer security issues, e.g. Ware, 1979 [WARE-79].

Department of Defense
Trusted Computer System Evaluation Criteria
15 August 1983.

Division C: Discretionary Protection.

Classes in this division provide for discretionary (need-to-know) protection and, through the inclusion of audit capabilities, for accountability of subjects and the actions they initiate.

Division B: Mandatory Protection

The notion of a TCB that preserves the integrity of sensitivity labels and uses them to enforce a set of mandatory access control rules is a major requirement in this division. Systems in this division must carry the sensitivity labels with major data structures in the system. The system developer also provides the security policy model on which the TCB is based and furnishes a specification of the TCB. Evidence must be provided to demonstrate that the reference monitor concept has been implemented.

Division A: Verified Protection

This division is characterised by the use of formal security verification methods to assure that the mandatory and discretionary security controls employed in the system can effectively protect classified or other sensitive information stored or processed by the system. Extensive documentation is required to demonstrate that the TCB meets the security requirements in all aspects of design, development and implementation.

USA Department of Defense TCSEC - 1983.

The resultant document was the 1983 TCSEC document, updated in 1985. The TCSEC sets out three fundamental security requirements summarised as *policy*, *accountability* and *assurance*. These requirements were combined into a set of security "**divisions**" and then further into "**classes**" within these divisions which would characterise computer system security in a succinct manner, as shown in the previous table.

Towards the late 1980s, however, these criteria were being augmented by other criteria developed by other nations, e.g. Canada, United Kingdom, Germany, The Netherlands, etc. for a number of technical and political reasons.In particular, 1990 saw the convergence of the work in France, Germany, the Netherlands and the United Kingdom into a set of "harmonised" criteria; the so-called Information Technology Security Evaluation Criteria or ITSEC [ITSE-90]. These were seen as a superset of the earlier TCSEC and expanded the concepts to emerging new IT products and systems. The main conceptual advances in the ITSEC were the:

- separation of the concepts of security "functionality" and security "evaluation" into distinct categories; and
- coverage of both "products" and "systems" in a single document set.

The evaluation or assurance criteria are set out as six separate criteria labelled E1 to E6. It should be noted that these evaluation level criteria are built into the divisions and classes of the earlier TCSEC. The ITSEC functionality criteria are likewise mapped into separate groups that firstly map the functionality of the TCSEC, called F-C1 to F-A1, while allowing for special functionality classes of high integrity (F-IN), data confidentiality (F-DC), etc. In ITSEC senses this paper examines the proposal that information products and systems need to meet a level of F-B1, E3 as a minimum to abide by the OECD and like guidelines or an evaluation level of EAL-4 in Common Criteria terminology.

1.5 Access Control/Mandatory versus Discretionary versus None

Gasser [GASS-88] set out, in his 1988 book "Building a Secure Computer System", some background for the underlying reasoning in this paper. He states:

> *"Until the early 1970s, it was not generally realised that two fundamentally different types of access control exist.* ***Discretionary access control*** *is the most common: users, at their discretion, can specify to the system who can access their files. ... Under* ***nondiscretionary*** *or* ***mandatory access control****, users and files have fixed security attributes that are used by the system to determine whether a user can access a file. The mandatory security attributes are assigned administratively (such as by a person called the security administrator) or automatically by the operating system, according to strict rules. The attributes cannot be modified by users or their programs."*

These concepts may be extended to object-oriented concepts whereby information technology professionals may associate *"methods"* with *objects* or *classes* whereby those methods must be compulsorily invoked whenever an object is referenced. However, as in the case above, the question as to who has responsibility for the determination of the rules for such methods again fits into the discretionary versus mandatory debate.

There has been suggestion that the early TCSEC discretionary "C2" class of assurance is good enough for information systems in the 1990s, particularly in the banking and finance, health care and commercial government systems area. Indeed Gasser [GASS-88] points out that:
"In practice, mandatory controls do provide a benefit over discretionary controls, even if Trojan horses are not a threat, in cases of accident or irresponsibility." [GASS-88. Pg. 62].

With the introduction of so-called "scripting languages", such as "JAVA", whereby programs may be transmitted over national and international networks for execution on willing host systems, the Trojan Horse threat has taken on a new significance. This again adds force to the argument that discretionary levels of security are now obsolete and moves to mandatory levels, essential since now a "user" by definition, may be any "applet" provider. In the JAVA case, at least, the JAVA language interpreter, usually integrated into a World-Wide-Web or Internet access program or "browser", must be guaranteed to enforce the strong "typing" requirements of the JAVA language, including restrictions to local data/input-output operations.

2. The OECD Principles

The OECD has detailed a set of nine "principles" which underpin the overall guidelines set. These are labelled as:

1. Accountability;
2. Awareness;
3. Ethics;
4. Multidisciplinary;

5. Proportionality;
6. Integration;
7. Timeliness;
8. Reassessment; and
9. Democracy

"Principles". Each principle is considered below in relation to overall computer security requirements and the "mandatory" security theme.

2.1 Accountability

> The responsibilities and accountability of owners, providers and users of information systems and other parties concerned with the security of information systems should be explicit.

OECD Accountability Principle

The essential part of this OECD requirement, and its highlight, is the requirement for the overall responsibilities to be **explicit**. This covers the *"owners, providers and users"* of the system. Such a set of requirements covering the people involved with an information system can only be met by the clear definition of central responsibility for the information resources under consideration. The "responsibilities" that are to be explicit need to be clearly defined, explained and *"apportioned"* as required. In turn these need to be enforced and accountability maintained. This requires the provision of a system wide audit facility to enable any form of accountability to be effective.

Now, the TCSEC Division C classes allow for *"discretionary (need-to-know) protection"* as well as some audit facilities for accountability of subjects in the system. However, for the system security to be explicit there needs to be a recognised system security manager capable of defining and enforcing such responsibilities and accountability. This is not possible at the discretionary level where individual users are responsible for the implementation of any security paradigms on an individual program and/or data files basis. The ability to processs a JAVA applet, the "product" of an unknown user is relevant here. At the TCSEC "C" level no system manager can make reasonable pre-evaluations of code. In particular, the ITSEC F-B1 functionality class enhances this requirement in relation to "channels" of communication between subjects, based on the earlier TCSEC "B1" class. If a channel allows for information of varying security requirements to be transmitted and received, in the same computer or across a network, then:

> *... it shall be ensured by the communications protocol that the recipient can completely and unambiguously reconstruct and pair the received data and attributes." [ITSE-91]*

This condition is simply not referenced at the TCSEC "C2" or lower class levels and appears as a necessary requirement in the decade of data networks to meet OECD Guidelines. Even within a single host.

2.2 Awareness

> In order to foster confidence in information systems, owners, providers and users of information systems and other parties should readily be able, consistent with maintaining security, to gain appropriate knowledge of and be informed about the existence and general extent of measures, practices and procedures for the security of information systems.

OECD Awareness Principle

Essentially this OECD principle requires that the overall security policy and its enforcement procedures and techniques be made known to "owners and providers". At the "Discretionary" division of TCSEC such awareness may not be possible since, essentially, each individual program and data base sub-system may be separately controlled by different groups and be subject to differing security principles.

Data and programs, at the "C" level, do not need to be "labelled" with system wide parameters. Moreover, in a distributed computing environment, with client/server programming systems involved and distributed object models of information system management invoked, it is impossible for individual sub-system "owners", usually the IT professional who developed the application, to understand and disseminate all security parameters to users of their sub-system. With the development of so-called "object request brokers (ORB)", whereby distributed information "objects" may communicate in an organised manner, it would appear that such security information needs to be incorporated into the ORB in such a manner that the ORB is itself protected from misuse and "tampering". In other words, this principle extends beyond the simple documentation of security practices in such documents as an "enterprise security manual" or the like, to the actual incorporation of security parameters into the information system itself.

2.3 Ethics

> Information systems and the security of information systems should be provided and used in such a manner that the rights and legitimate interests of others are respected.

OECD Ethics Principle

The rights and legitimate interests of others simply means that system users need to be identified to the information system and global security parameters set. These parameters should be regarded as being "system" or "enterprise" wide and not just associated with individual applications or sub-systems that operate on an information system. In particular, the overall information system may need to be consistent with any national or regional laws affecting the privacy of individuals and the responsibilities for "data protection" that may exist. Such laws and guidelines are, in a computing sense, a set of "global rules" that must exist in the overall system itself. It is infeasible to incorporate them individually into every separate application that operates on the information system, particularly in a distributed system. This has significance when "scripting languages", e.g. "JAVA", Telescript, etc. are used to dynamically create applications that may be transmitted over a data network for execution on a remote host system with resultant data/information re-transmitted to the originator of the "script". The nature of such "scripts" ("applets") cannot be predicted by IT professionals at the time that an information system is created and thus appropriate security parameters must be set that are global in nature and which meet the ethics principle. Mandatory security, with appropriate enforced labelling of data and programs, is the only technology capable of meeting this need.

2.4 Multidisciplinary

Once it is agreed that diverse viewpoints in relationship to an enterprise's information system must be taken into account, the need for a global information security policy that is enforced becomes essential. Any resultant "measures, practices and procedures" need to be reliably enforced over the whole system requiring that mandatory security features be provided in the system to allow for such parameters to be centrally defined and monitored. This essentially rules out the use of "discretionary" systems as each application group operates "on its own" without consideration, in principal, for other groups. It is the responsibility of the C class system to "isolate" such groups and application sets. The "mandatory" scheme enforces a multidisciplinary approach on system security management.

> Measures, practices and procedures for the security of information systems should take account of and address all relevant considerations and viewpoints, including technical, administrative, organisational, operational, commercial, educational and legal.

OECD Multidisciplinary Principle

2.5 Proportionality

This principle implies that IT professionals, in creating an information system, have performed appropriate levels of risk analysis and assessment prior to placing the system in operation. While this may be uncommon such analysis is the only way to determine the level of security technology needed to provide adequate safeguards for the system. There has been a general opinion that computer systems that implement "mandatory" access control and like services are too expensive in terms of cost and resource requirements with associated degradation of overall system performance. This can now be disputed with a larger number of systems being evaluated at the so-called "B1" level of trust according to the "Orange Book" while demonstrating minimal performance degradation, e.g. Secure UNIX SVR4.1, etc. Arguments on the basis of cost against use of mandatory, trusted technology are becoming less tenable as systems generally move to this level. There is, however, a problem at the personal computer/workstation level with mass/commodity system software. Incorporation of add-in security technology to raise the level of these systems to "B" (mandatory) could be a problem, particularly where such systems may be incorporated into an enterprise or cross enterprise distributed information system.

> Security levels, costs, measures, practices and procedures should be appropriate and proportionate to the value of and degree of reliance on the information systems and to the severity, probability and extent of potential harm, as the requirements for security vary depending upon the particular information systems.

OECD Proportionality Principle

2.6 Integration

This principle gives a clear direction towards overall mandatory security of information systems. In a discretionary system it is not possible to coordinate overall security parameters under the control of a security manager who can be responsible for such coordination and integration. If IT professionals develop and implement their own security schemes on an individual sub-system basis, it would appear to be impossible to create a coherent system of security even if security parameters for an enterprise are clearly set out in appropriate system development documentation. In particular, levels of enforcement may vary across individual application sub-systems.

> Measures, practices and procedures for the security of information systems should be co-ordinated and integrated with each other and with other measures, practices and procedures of the organisation so as to create a coherent system of security.

OECD Integration Principal

2.7 Timeliness

> Public and private parties, at both national and international levels, should act in a timely co-ordinated manner to prevent and to respond to breaches of security on information systems.

OECD Timeliness Principle

> The security of information systems should be compatible with the legitimate use and flow of data and information in a democratic society.

OECD Democracy Principle

In many cases, computer and data network security systems aim at the prevention of security related events that may compromise the overall system. There has been growing interest in the problems of recovery after a security event has occurred and the incorporation of such recovery technologies and procedures into information system security schemes. With a mandatory philosophy such recovery facilities can be centralised and controlled whereas with any security level below this individual security recovery processes may need to be taken for each and every application sub-system that operates within an overall information system. This could be a major problem in a distributed system where individual host computers may be physically separated and be under the control of different management group in an enterprise or across co-operating enterprises, such as in the case of electronic data interchange (EDI) schemes.

2.8 Reassessment

> The security of information systems should be reassessed periodically, as information systems and the requirements for their security vary over time.

OECD Reassessment Principle

Periodic assessment of overall information system security becomes only feasible with centralised systems of security management and enforcement. Moreover, if changes are needed as a result of such reassessment then it is totally impractical to mandate changes to all application level programs and data structures at the discretionary level of system architecture. Centralised security features and their enforcement dictate the use of mandatory security services at the operating system level for all hosts in a distributed computing network, regarded as the norm for information systems into the 21st century. This does, however, mean that research is needed into the dissemination of such changes in security parameters between trusted hosts in a computer network to mirror security changes in individual mandatory access control and system security schemes in connected computer hosts.

2.9 Democracy

This requirements could be best considered in relation to the reassessment principle. Overall system security requirements must be measured against legitimate legal rights in a democratic society. For this to be possible, overall responsibility for system security management must be identifiable and obvious. This means that if security parameters are left to individual developers of sub-systems and applications in the information system it may become impossible for this principle to be implemented and such implementation to be checked in real system cases. Mandatory information system security schemes could assist in implementation and management of this principle.

3. Conclusions

There is, however, a problem. This paper has argued that the mandatory (B level functionality) specifications of the TCSEC and ITSEC provide a base for definition of "commercial-level" functionality classes that meet the needs of emerging security guidelines and legislation internationally at the levels of F-B1, E3 for ITSEC and B1 for TCSEC and equivalent Common Criteria levels. By contrast the probability that manufacturers of computer hardware, system software and "generic" application systems, as well as necessary intermediate software systems such as network protocol sets, graphical user interfaces, etc., will embrace such security and quality features soon, is very low. This was alluded to in the 1991 report of the United States National Research Council (NRC) entitled "Computers at Risk" [NRC-91], Page 145, as follows:

> *"The slow growth of the market for secure software and systems feeds vendors perceptions that its profitability is limited. Both high development costs and a perceived small market have made secure software and systems development appear as a significant risk to vendors. Moreover, a vendor that introduces a secure product before its competitors has only a year or two to charge a premium. After that, consumers come to expect that the new attributed will be part of the standard product offering. Thus the pace of change and competition in the overall market for computer technology may be inimical to security, subordinating security-relevant quality to creativity, functionality, and timely releases or upgrades. These other attributes are rewarded in the marketplace and more easily understood by consumers and even software developers."*

However, the problems of incorporation of safety features and the reliability of those features into products and systems has long been recognised in other industries such as the car industry, fire prevention sector, etc. Car manufacturers did not incorporate seat belts in cars as a standard offering until it became mandatory under law. Office building proprietors did not include fire extinguishers and sprinkler systems until, again, it became compulsory by law. There is no reason to believe that the computer and telecommunications industries are any different, as has been indicated by the NRC report above. Even consumers themselves normally do not consider safety and security unless compelled to do so, at least beyond fundamental and basic levels, e.g. door locks, car locks, etc. as evidenced by the lack of penetration of smoke detectors in buildings, homes, etc.

The OECD Guidelines and any associated national responses to them, in the form of computer and data network security legislation, could assist in changing the scene, as it did for the car industry. The **mandatory security** features of the TCSEC and ITSEC and, in particular, a rework of these for commercial level requirements under the Common Criteria, could be incorporated into "mainstream" computer systems, particularly distributed systems. These could then be sent to meet growing world requirements on management to comply with the OECD Guidelines and associated national developments of these.

4. References

BSI-93 British Standards Institute, 1993.
"A Code of Practice for Information Security Management"
ISBN 0 580 22536 4.

CC-96 Common Criteria, Vers. 1.0.
Common Criteria Implementation Board (CCIB),
http://csrc.nist.gov/nistpubs/cc

CLAR-87 Clark, D.D. and Wilson, D.R.
"A Comparison of Commercial and Military Computer Security Policies"
in Proceedings of the 1987 IEEE Symposium on Security and Privacy,
Pg. 184-195
IEEE Computer Society, USA, 1987.

GASS-88 Gasser, M.
"Building a Secure Computer System"
Van Nostrand Reinhold Company, New York, USA, 1988.
ISBN 0-442-23022-2.

ITSE-91 Information Technology Security Evaluation Criteria (ITSEC),
Version 1.2, 1991
United Kingdom, Germany, France, The Netherlands.

LIPN-82 Lipner, S.
"Non-discretionary Controls for Commercial Applications"
in Proceedings of the IEEE 1982 Symposium on Security and Privacy"
IEEE Computer Society, 1982.

NRC-91 National Research Council, U.S.A.
"Computers at Risk : Safe Computing in the Information Age"
National Academy Press, U.S.A., 1991
ISBN 0-309-04388-3.

OECD-80 Organisation for Economic Co-operation and Development (OECD)
"Guidelines on the Protection of Privacy and Transborder Flows of Personal Data", 23 September 1980.
OECD 1981.

OECD-92 Organisation for Economic Co-operation and Development (OECD)
"Guidelines for the Security of Information Systems", 26 November 1992
Document : OECD/GD(92)190.

WARE-79 Ware, W.