Security Accreditation, Management and Monitoring - Getting the Balance Right!

Author

Peter J Fischer, Asset Security Manager, Government Communications Headquarters, Cheltenham, UK
Tel: +44-1242-221491, ext.2868
Fax: +44-1242-226816
Email: fischer@which.net

Abstract

Traditional methods of security accreditation in the Government classified arena are outdated. They are becoming increasingly ineffective in maintaining security, irrelevant and damaging to the effectiveness and efficiency of IT systems and the organisations they serve.

It is important to move towards a genuine risk-management approach to IT security. Whilst accreditation still has a part to play, it should be reduced in scope and more focused. This will release resources to concentrate on the important tasks of monitoring and auditing IT security of systems and networks in operation. Intelligent penetration testing will form an important part of any monitoring regime.

To be effective this approach will rely on close co-operation between IT security professionals, developers and managers. Responsibilities must be shared and an atmosphere of partnership and co-operation developed

Keywords

Accreditation; Certification; Trusted Systems; Network Security; Enterprise Security Management; Penetration Testing; Security Health Checks.

Security Accreditation, Management and Monitoring - Getting the Balance Right!

by
Peter J Fischer MBCS

Introduction

1. Computer Security (CompuSec) in the classified arena of Government has traditionally focused almost exclusively on the accreditation (certification) of a system on introduction to operational use. The exercise of accreditation has evolved into a bureaucratic, clerical exercise centred on the production of a range of documents - security policies, plans and procedures - which are submitted to the accreditation authority for review and, ultimately, approval.

2. Government security authorities have also encouraged the use of Trusted Products to implement countermeasures in support of confidentiality requirements, often using guidance documents such as the Yellow Book and CESG Memorandum No. 10 almost as bibles to assess the risk to IT systems and networks and translate these into a TCSEC or ITSEC value.

3. This approach has its roots in the stable, mainframe environment of the 1970s and 1980s, when networking was supported by proprietary protocols which tended to preserve system boundaries. It is becoming increasingly dated, inadequate for and irrelevant to the modern IT environment because of:

a. The evolution of TCP/IP as the universal protocol set for networking.

b. The inability of many Trusted Products to meet operational and business requirements.

c. The dynamic development of more powerful and flexible IT products.

d. The failure to reflect and respond to change.

Accreditation of Classified Systems - An Historical Perspective

4. In the days when, first dumb terminals, and later dedicated terminals with some intelligence were connected to mainframe computers, or even mini-computers, using proprietary communications protocols it was relatively easy to define the boundary of a system. The accreditor therefore had an easily defined entity to assess from a security perspective and within which to identify security threats, define security requirements and approve countermeasures, thereby accrediting the system.

5. This situation has changed beyond recognition with the evolution of TCP/IP as the *de facto* universal networking protocol. The security target for new server systems and applications introduced to a TCP/IP network environment can no longer be clearly separated from all the other facilities on the network for purposes of accreditation. Indeed, it could be argued that such developments are not, and should not be viewed as, new systems but merely a development or enhancement of a much wider system - to paraphrase the Sun assertion, the system has become the network. In this new environment, attempts to apply outdated accreditation procedures are becoming increasingly questionable and irrelevant, adding less and less value in both security and business terms.

Trusted Systems

6. As my colleague, Michael Stubbings, asserted in his paper presented to the 19th National Conference, in Government, as in commerce and industry, powerful and flexible IT systems are needed to improve efficiency and effectiveness. Moreover, we in Government owe it to the nation, our employers and ourselves as professionals to ensure that we operate as efficiently and effectively as possible. All too often, a rigid approach to security, and to Trusted Systems in particular experience has not been in accord with the business strategy of classified communities within Government, has incurred excessive and unnecessary development costs, and resulted in systems which do not deliver the requisite benefits to the user. In extreme cases, valuable IT projects have been emasculated, cancelled or strangled at birth in the name of security.

7. The problem centred on a risk avoidance approach by security accreditors whose focus was on the integration of rigorous technical countermeasures within systems which could be guaranteed to prevent security compromises throughout the life of the system. The recognition is beginning to dawn that this aim is not achievable within a multi-functional, flexible, powerful and expanding IT facility. In practical terms, the risks cannot be avoided, but must be minimised and managed effectively and continuously.

8. There is another inherent danger in the initial, one-off approach to security accreditation. In the UK, where Trusted Systems have been accredited for operational use in the classified arena, there is evidence that this has discouraged a sense of ownership of security issues by project managers and system managers and engendered a false sense of security amongst users and managers. Systems evolve, threat scenarios change, but once a system has become operational, few accreditors review its security. Yet many managers and users, used to working in a closed community, do not recognise the security dangers and assume, naively, that as the system has been accredited it is automatically "safe" through life.

9. Whilst there are many Trusted Systems in operation in which trust has been placed unwisely, or where security constraints have impacted performance and benefits significantly and unnecessarily, there are shining examples where the balance between the user requirement and security has been struck, and where security is properly managed and monitored throughout the life of the system. We need to move to a situation whereby the latter is the norm and the former is outlawed.

Trusted Products

10. Trusted Products have played a major role in the security of classified systems and networks, and will continue to do so. But to provide the degree of security needed in the modern, networked, distributed IT environment, major culture changes are needed throughout the whole IT security community which serves Government. In particular we need:

a. Improved strength of mechanisms, ie vendors need to be encouraged to build more rigorous security mechanisms into standard, function-rich products.

b. High assurance products developed and integrated into systems where they are <u>really</u> necessary and add value without unnecessary constraint (eg firewalls).

c. <u>Everyone</u> to recognise that risk cannot be avoided, but must be managed actively throughout the life of the system or network.

11. The lead in respect of the first two must rest with vendors and national authorities working together. Products such as Operating Systems, DBMSs, Network Management Systems must continue to be developed to meet the business drivers of functionality and efficiency, but integrating , for example, more rigorous mechanisms for authentication which are less easily subverted than the current industry standard of multi-use passwords. In

doing so, vendors need to be supported by security authorities, who must recognise that such an approach can never result in products which avoid the risk. There will be vulnerabilities which will be exploitable throughout the life of the product, and these vulnerabilities have to be managed - it is not feasible to even try to design them out.

12. There will remain a (small) requirement for high assurance products to provide specific services to the classified Government community, in much the same way as high-grade cryptography products have been developed for many years to protect Government classified communications. Areas which spring to mind as candidates include the development of high-assurance firewalls (the classified community cannot hide from the Internet indefinitely).

Managing Security in the Modern IT Environment

13. Firstly it must be recognised that security accreditation based on procedures which are largely paper-based and which are performed on a once-off basis when a system or facility is introduced into operational service add little value to the security process. It is important that the process of building security into systems and applications must be recognised as a shared responsibility, between the accreditor - who states the requirement and advises on their implementation - and the project manager and system designer - who accepts responsibility for meeting the security requirement. This process should enable security resources to be released to address other aspects of IT security, especially monitoring the security and the security management of systems and networks.

14. This does not mean that the security authorities should be actively involved in day-to-day system and network security management issues. To the contrary, it remains important that these functions are performed by the same individuals who undertake operational management functions. But again, as with project managers and system designers, system and network managers must recognise the importance of security and undertake these duties conscientiously, working in partnership with the security authorities.

15. In this new, security-aware management culture, it is important to recognise that security issues transcend the outmoded, mechanical, procedural security functionality as specified in generations of Security Operating Procedures. Managers must develop and maintain an awareness of security issues which relate specifically to their environment and which develop and evolve continuously.

16. There is another important issue to be considered in the context of security management. In the majority cases, partly because of the accreditation process, security of systems and networks has been addressed and developed on a case-by-case basis. This has led to fragmentation and inconsistency. With the expansion of IT facilities and networks, it is essential that this trend is reversed and the classified IT community moves towards Enterprise Security Management.

Security Audit and Monitoring

16. The role of the security authorities in this whole process is to set and review policy and to monitor the continuing effectiveness of its implementation in practice. This should not be seen as purely a policing role, but a genuine co-operative process between IT security and operations.

17. If we are moving towards a genuine culture of risk management, the role of active monitoring is likely to be crucial. Risk management in the modern IT environment must involve the acceptance that it is not possible to design out all vulnerabilities or implement security mechanisms with a degree of rigour that guarantees security forever.

18. Active security monitoring should involve a variety of processes, including security inspections, system audits and intelligent penetration testing, often referred to as “security healthchecks” in the UK. These can

provide a valuable source of information to security authorities and, possibly more importantly, to senior corporate management, who are sometimes reluctant to accept that vulnerabilities exist and can be exploited.

19. Regrettably, there has been much hype within the IT security media about the employment of "reformed" hackers and crackers for this work. Fortunately, such a high risk option is not necessary as there is a growing number of reputable players in this field. Within the UK, Government organisations such as the Communication-Electronics Security Group (CESG) and the Defence Evaluation and Research Agency (DERA) provide an excellent, professional service in performing intelligent penetration tests and undertaking "health checks" of systems and networks; several reputable commercial companies provide a similar service. In the US, companies such as WheelGroup Corporation have gained an international reputation in this field.

Conclusions

19. Traditional methods of security accreditation in the Government classified arena are becoming increasingly ineffective, irrelevant and damaging. It is important to move towards a genuine risk-management approach to IT security.

20. Whilst accreditation still has a part to play, it should be reduced in scope and more focused. This will release resources to concentrate on the important tasks of monitoring and auditing IT security of systems and networks in operation.

21. To be effective this approach will rely on close co-operation between IT security professionals, especially Infosec accreditors and inspectors, IT architects, system developers and managers. Responsibilities must be shared and an atmosphere of partnership and co-operation developed.

22. Whilst there is evidence of movement to these ends, we must ensure that progress is maintained and, if possible speeded up. We cannot afford to fail!

Peter J Fischer MBCS