Liu, Vicky and Caelli, William J. and May, Lauren J. and Croll, Peter R. and Henricksen, Matthew P. (2007) Current Approaches to Secure Health Information Systems are Not Sustainable: an Analysis. In Proceedings Medinfo 2007, pages P399-P399, Brisbane, Australia.

Current Approaches to Secure Health Information Systems are Not Sustainable: an Analysis

Vicky Liu, William Caelli, Lauren May, Peter Croll, Matt Henricksen

Information Security Institute, Queensland University of Technology, Australia

Abstract

This paper proposes a viable IT-based solution for ensuring the privacy and security of sensitive information in contemporary Health Information Systems (HIS).

Keywords

Trusted systems, Information assurance, Privacy, MAC, HIS.

Introduction

In today's society Information, Computer and Telecommunications technologies (ICT) are increasingly entrenched as information infrastructures for the majority of essential services in leading countries such as Australia, the UK and the USA. ICTs are being designed and deployed to process, transmit and store health information in various e-health systems globally. These systems play a significant role in the potential improvement of quality and productivity in the health sector.

In order to manage healthcare stakeholders' expectations of these systems, governments have initiated e-health blueprints which provide guidelines to the developers of HIS. These guidelines take into account the interests of all stakeholders in the health sector.

This paper is particularly interested in the implementation of HIS from an information security aspect: the protection of personal privacy and security of electronic patient records. Current approaches to information security in HIS are, in the opinion of the authors, not sustainable. This paper proposes a viable ICT solution which can reliably provide appropriate levels of secure access control for the protection of sensitive health data in HIS.

Access Control in ICT

Access control is one of the fundamental security mechanisms used to protect computer resources; in particular in multi-user and resource-sharing computer environments such as contemporary HIS. The lack of adequate access control management in such systems has been demonstrated on numerous occasions in recent history: the privacy invasion scandal at Australia's Centrelink [1], the lack of adequate safeguards in the UK NHS patient records system [2], and the significant IT security weaknesses identified in the USA HHS information system [3]. These types of breaches have the potential for inflicting, and do inflict, major harm on consumers and providers alike. The issue of providing suitable access control in such systems is not an insurmountable one. This paper proposes a viable solution to this issue.

The two traditional types of access control modes are Discretionary Access Control and Mandatory Access Control:

The **Discretionary Access Control (DAC)** mechanism allows the owner of information to grant access permissions to other users or programs at his/her discretion without the system administrator’s knowledge. Such a policy does not provide the actual 'owner' of the system fully centralised access control over the organisational resources. DAC mechanisms are fundamentally inadequate for strong system security because the owner of the system does not have access control over the objects (files) on the system.

The **Mandatory Access Control (MAC)** mechanism provides the ability to limit access to only legitimate users. Ferraiolo et al [4] underscore that MAC is necessary when the provision of a truly secure system is required. Access permission to information is determined by the user’s security clearance compared to the security level of information determined by the system. This is also known as a multi-level security (MLS) policy, which was first introduced by Bell and LaPadula (BLP) [5] .

Role-Based Access Control (RBAC) is complementary to both DAC and MAC techniques. RBAC enables easier management by ensuring finer granularity in the access system.

The majority of current information systems which manage access control are DAC-based allowing for wide implementation of commodity software and hardware. Examples are Microsoft Corporation’s Windows systems, open-source systems such as Linux and the original Unix system. These are general-purpose systems intended for use in as many applications as possible. In the healthcare sector, HIS MAC-based systems are more appropriate to, and capable of, satisfying the specific requirements of privacy and security of information.

In technical computing terms an application program resides atop a number of sub-systems, one of which is the operating system (OS) which effectively controls what the hardware does. The security of an application program is restricted by the strength of the security that the OS allows. DAC and

MAC mechanisms are enabled at the OS level as well as higher levels including data network management and the database management systems for the application.

Our Approach

ICT is now sufficiently advanced that a MAC-based electronic healthcare management system is feasible. Our research to date has indicated that current OS structures need to be updated for HIS needs. The Health Informatics Access Control (HIAC) model is our approach to overcoming many of the privacy and security issues which have plagued previous attempts at electronic health management systems. The HIAC is based on the MAC type of OS which primarily satisfies the requirement for confidentiality of records (this is a major impediment in current and previous systems). The HIS is then developed atop the trusted OS.

For general applications, currently available products that support the MAC principles of trusted OS include "Red Hat Enterprise Linux (RHEL) Version 5, "Fedora Core 6", and "Sun Microsystems Solaris 10 with Trusted Extensions Software". The HIAC model exploits the privacy- and security-enhancement features of such trusted OS in the healthcare environment. The end result is a dedicated trusted HIS which satisfies all privacy and security requirements.

To determine the practical viability of a HIAC model for HIS a demonstrator, based on the Security Enhanced Linux (SELinux) OS with MAC and RBAC approach, was built [6] The HIAC model is necessarily MAC-based accompanied by RBAC properties for flexibility and a refined level of granularity. This degree of simultaneous control and flexibility is not achievable with DAC, RBAC or MAC individually.

The MAC-based system can provide the ability to limit access to only legitimate authorised users. In general, the organisational security policies can be defined by the CEO/CIO. Access privileges are determined by the data custodians. The HIAC profiling mechanism allows for the system administrator to configure the organisational access policies defined and determined by the CEO/CIO and the data custodian. With MAC the access privileges of all users are equally bound by the policy, not set by the discretion of the file/program owners as with DAC. The internal adversary or disgruntled employee will not be able to access health information inappropriately or even through feeding information to an external adversary.

The MAC mechanism can protect the system from malicious or flawed applications which can potentially damage or destroy the system and its information. This can prevent an external adversary penetrating the system by exploiting Trojan Horse attacks, viruses, malware, social engineering or other illicit means to gain total access control or to tamper with audit systems. The HIAC model includes the principle of least privilege and also enforces domain separation through the use of the protected zones known as 'sandboxes' within Redhat's SELinux. These help prevent applications interfering with each other such that an unauthorised user cannot gain overall control of the system as with DAC.

HIAC incorporates RBAC which complements contemporary MAC systems by ensuring more flexibility over the more traditional MAC standalone systems. With RBAC Doctor X and Nurse Y are appointed into a role-type, for example Doctors and Nurses respectively. Access permissions are associated with these roles. In practice this approach gives more flexibility than in the traditional MAC where accesses are granted to individual persons.

In general HIAC provides for maximum flexibility within a strongly secure environment. This means achieving a balance between security needs and flexibility of implementation, which is primarily determined from a privacy risk assessment. For example HIAC provides the flexibility of having an emergency override function by switching to the emergency policy in emergency circumstances. Full auditing of the system deters potential abuses of this flexibility.

Conclusion

Current moves toward Web-based identity and authentication structures present major challenges where such structures are not based on highly trusted OS. The majority of OS in use today are DAC-based in which there are no inherent privacy and security features. All applications and supporting software which necessarily reside atop these untrusted operating systems are also untrusted and therefore vulnerable from a privacy and security viewpoint.

This paper contends that it is both timely and desirable to move electronic HIS towards privacy- and security-aware applications that reside atop trusted computing-based OS. Such systems have the real-world potential to satisfy all stakeholder requirements including modern information structures, organizational policies, legislative and regulatory requirements for both healthcare providers and healthcare consumers (privacy and security), and flexible operational demands in HIS.

This paper emphasises the need for well-directed research into the application of inherent privacy- and security-enhanced operating systems to provide viable, real-world trusted HIS. The authors propose an HIAC model which has the potential to fulfil these requirements.

References

[1] Sharanahan D and Karvelas P, Welfare workers axed for spying, The Australian, issued on 23/08/2006, http://www.theaustralian.news.com.au/story/0,20867,20223075-601,00.html accessed 23/08/2006

[2] Leigh D and Evans R, Warning over privacy of 50m patient files, Guardian News and Media Limited, issued on 01/11/2006, http://society.guardian.co.uk/health/news/0,,1936403,00.html accessed 01/11/2006

[3] GAO, Information Security: Department of Health and Human Services Needs to Fully Implement Its Program. 2006 United States Government Accountability Office

http://www.gao.gov/new.items/d06267.pdf accessed 20/11/2006

[4]Ferraiolo DF, Kuhn DR, and Chandramouli R, Role-Based Access Control. 2003, Boston.London: Artech House.

[5]Bell DE and LaPadula LJ, Secure Computer Systems: Mathematical Foundations and Model, The Mitre Corporation, 1973

[6]Henricksen M, Caelli W, and Croll PR. Securing Grid Data Using Mandatory Access Controls. in *to appear in 5th Australian Symposium on Grid Computing and e-Research (AusGrid 2007)*. 2007. Ballarat Australia.