

Open Trusted Health Informatics Structure (OTHIS)

Vicky Liu, William Caelli, Lauren May and Peter Croll

Faculty of Information Technology & Information Security Institute

Queensland University of Technology

PO Box 2434 Brisbane QLD 4001, Australia

v.liu@qut.edu.au w.caelli@qut.edu.au l.may@qut.edu.au croll@qut.edu.au

Abstract

The potential for development and deployment of trusted health information systems (HIS) based upon intrinsically more secure computer system architectures than those in general use, as commodity level systems, in today's marketplace is investigated in this paper. A proposal is made for a viable, trusted architecture for HIS, entitled the "Open Trusted Health Informatics Structure (OTHIS)", based upon a set of separate but connected trusted modules. OTHIS addresses privacy and security requirements at all levels in an HIS. In this paper, we are concerned with the role of trustworthy access control mechanisms in HIS architectures. Our proposed OTHIS architecture gives direction on how trustworthiness in HIS can be achieved.

Keywords: information assurance, security for health systems, access control, mandatory access control, trusted systems, information security and privacy

1 Introduction

Graauw (2005) clearly set the scene for the emergence of Web Services oriented implementation of next generation health information systems. While coordination of data exchange must play a vital role in any national electronic health record scheme, the overall information assurance of the system cannot be left to the associated messaging system alone. For example, Graauw emphasizes that "... all messages are exchanged between a provider HIS and a healthcare information broker (HIB), which in turn may send the data contained in those messages to other healthcare parties." The importance of the assurance of all intermediary computer systems and associated databases cannot be underestimated as these may quickly become the "weakest link". The paper clearly acknowledges this in the following statement in its conclusion: "*It is possible to build a reliable and secure framework for sending medical data over the Internet ... provided all transport nodes are reliable.*" This provision appears to be noted in much of the research conducted to date which is based around the assured transportation of electronic medical records. This places great emphasis again on the need for high trust computer

systems to act as intermediary nodes at all points in the network, and particularly at any integration or brokerage points.

Not all computer systems however are the same from a security viewpoint. We propose an overall trusted HIS architecture by which appropriate computer and network components may be evaluated and selected. This is the fundamental concept of any architecture, namely the ability to select appropriate components or products so as to create a highly secure system overall. The architectural work described in this paper presents such selection criteria.

It has been long acknowledged that an application program can be no more secure than the software libraries and other subsystems it uses and depends upon. These in turn can be no more secure than any "middleware" that they may use, nor the operating system upon which they depend. Finally, all these depend upon the underlying hardware and firmware, including any driver and device support subsystems. In the creation of real healthcare related information systems, however, the question still arises of just where appropriate security, control and management (SCM) services and mechanisms should exist in these systems to provide overall information assurance. The question then devolves into a discussion on granularity and the "intelligence" that exists at each layer in a real system. This has been a topic of research and discussion for well in excess of thirty years. With the propagation of the "Open Systems Interconnection (OSI)" model in the early 1980s some formality entered that discussion. The OSI seven-layer model is well known and acknowledged as a base for categorisation of cross computer platform services as shown in Table 1: ②. The top two layers, Layer 6: the "Presentation Layer" and Layer 7: the "Application Layer", would appear to play a major role if more "fine-grained" levels of control are required, particularly in relation to HIS based around distributed computer systems. For example, under OSI it was accepted that Layer 6 would provide the following services to an application sitting above it in Layer 7:

- Data formatting – including translation between different character and even computer "word" coding schemes such as ASCII, EBCDIC, UniCode, "little-end" vs "big-end" addressing, etc.; encryption and decryption services at an appropriate level of granularity ("selective field encryption"); etc.
- Provision of any compatibility requirements for the operating systems on the computers connected via the OSI scheme, and

Copyright © 2007, Australian Computer Society, Inc. This paper appeared at the Australasian Workshop on Health Data and Knowledge Management (HDKM 2008), Wollongong, NSW, Australia. Conferences in Research and Practice in Information Technology, Vol. 80. Ping Yu, James R. Warren, John Yearwood and Jon D. Patrick, Eds. Reproduction for academic, not-for profit purposes permitted provided this text is included.

- Encapsulation of application level data into appropriate blocks needed for transmission.

1.1 Security Goals for the Health Sector

The security goals for the health sector incorporate data management and control as a fundamental requirement. Indeed it is the protection of so-called “data at rest” that may be considered, from experience over the last five years or so, to be the single major security factor in the protection of health information systems. The issues of security and privacy of data in transit have been largely solved through the use of advanced cryptographic processes and procedures. Factors such as cryptographic key management with associated data communications protocols and message formats, such as those involved in the widely used and accepted “link-level encryption” based Secure Sockets Layer (SSL)²/Transport Layer Security (TLS)³ scheme, have been incorporated into such processes. These goals, for example, have been clearly defined in the statement of mission of Australia’s NEHTA⁴ as follows:

- *Improving the quality of healthcare services, by enabling authorised clinicians to access a patient’s integrated healthcare information and history, directly sourced from clinical notes, test results and prescriptions using standardised clinical data formats and terminologies.*
- *Streamlining multi-disciplinary care management, enabling seamless handovers of care by ensuring efficient electronic referrals; authorised access to up-to-date clinical opinions and patient healthcare histories via shared patient health records; and fast, secure mechanisms for directly exchanging important notifications between healthcare providers.*
- *Improving clinical and administrative efficiency, by standardising certain types of healthcare information to be recorded in eHealth systems; uniquely identifying patients, healthcare providers and medical products; and reforming the purchasing process for medical products.*
- *Maintaining high standards of patient privacy and information security.*

Requirements 1 and 4 of these NEHTA statements clearly emphasise the importance of creating a complete, usable and implementable security architecture for HIS on an end-to-end basis. Moreover, NEHTA also recognises that

² SSL, designed by Netscape, is a commonly used protocol for endpoint authentication and communications privacy using cryptography on the Internet
http://en.wikipedia.org/wiki/Secure_Sockets_Layer accessed 2/09/2007.

³ TLS, designed by IETF, is a non-proprietary protocol. It is derived from SSL and is almost identical to SSLv3.
http://en.wikipedia.org/wiki/Transport_Layer_Security accessed 2/09/2007.

⁴ NEHTA (National E-Health Transition Authority) was established by Australia’s Federal Government in 2005 to oversee the introduction of a system of national electronic health records.

privacy perceptions of the Australian community play a major role in ensuring the success of e-health systems (NEHTA 2006).

These factors are similarly emphasised in the USA through that country’s 1996 HIPAA (*Health Insurance Portability and Accountability Act*), issued by the USA’s Department of Health and Human Services (CMS 2004). The USA government intends to reform its national healthcare system with the goal of improving the effectiveness and efficiency of healthcare operations whilst assuring that health information remains private and secure. Achieving the security goals for HIS is a critical factor in the successful implementation of e-health initiatives.

1.2 Scope and Assumptions

The theme of this paper is in alignment with a number of specified topics within the scope of the conference including architecture of health information systems, privacy protection and the overall security/assurance of health systems. Appropriate data security management involves the protection of such data in storage, during processing and when transmitted. The proposed OTHIS structure addresses all of these areas. This paper focuses on the security and protection of data in storage or under processing parts of the OTHIS overall structure.

Our architecture assumes that the basic hardware and operating systems of all connected nodes in a healthcare information systems network are trusted and secure. We submitted that any such computer systems participating in an HIS must conform to the “Labelled Security Protection Profile (LSPP)” of the internationally accepted information systems security evaluation standard, the Common Criteria (CC)⁵ under international standard IS 15408. Appropriately, the CC’s LSPP embraces both Mandatory Access Control and Discretionary Access Control policy rules and sets strict access limitations on both users and data objects. In addition, a product or system meeting the LSPP provides better resistance to unauthorised access to the system from either internal or external parties. MAC and DAC are described in later sections.

Trust in network operations through health informatics network security (HINS) rests completely upon trust in health informatics application security (HIAS) and health informatics access control (HIAC), otherwise the security of messaging becomes futile. These three aspects of the OTHIS philosophy are discussed later in this paper. The necessary messaging and network structures (HINS), as part of this overall OTHIS philosophy, are explored in forthcoming papers.

⁵ CC, or the “Common Criteria” set is an international standard for creating information systems and products’ security specifications and for performing security evaluations. The CC provides a common set of requirements for the IT security of a product and system under the distinct categories of “functional requirements” and separate “assurance requirements”.

2 Related Work

Web Services (WS) and Service-Oriented Architecture (SOA) concepts and implementations are proliferating. The WS application model promises to add functional and assessment complexities to the overall information assurance problem by weaving separate components together over the Internet to deliver application services through such methodologies as software “mashups” and the like. These techniques place full trust in the underlying components that are combined into the overall system in a situation where the provenance of those underlying components may not be known.

NEHTA recommends using an SOA approach to the design of healthcare application systems and the use of “Web Services” as the technology standards for implementing secure messaging systems (NEHTA 2005). NEHTA argues that development of information systems around WS technology is the direction in which the ICT industry is heading as well as being accepted as best practice for the design of scalable distributed systems today. The SOA approach is claimed to lead to more reusable, adaptable and extensible systems over other techniques. In particular, NEHTA supports the concept that WS technology has gained notable attention within the ICT industry and its use is extending in both popularity and market penetration.

NEHTA work programs for an e-health interoperability framework include Clinical Information, Medicine Product Directory, Supply Chain Efficiency, eHealth Policy, Clinical Terminologies, Individual Healthcare Identifiers, Healthcare Provider Identifiers, Secure Messaging, User Authentication and Shared Electronic Health Record Specifications. NEHTA focuses on exchanging clinical information by electronic means securely and reliably. This may be achievable at the data communications link level by using secure messaging technology. The fact is however that the associated and critical health information computer systems will be openly connected to the Internet, and thus be exposed to “cyber-attacks”. This exposure has not been prevalent before. In this Internet connectivity environment, the issues of data “at rest” and “under processing” within a specific operating system are far more critical, as is evidenced by any cursory examination of illicit penetration of computer systems connected to the Internet globally. A complete architecture is needed, therefore, and not one that involves just a secure messaging system alone. OTHIS addresses the privacy protection and security for health systems in a holistic and “end-to-end” manner.

3 Our Approach

3.1 Architectures of HIS

A modern HIS architecture would normally consist of many subsidiary structures such as health application services, middleware-based functions, database management systems (DBMS), data network access and control systems, computer operating systems (OS) and hardware as shown as in Table 1: ③. Many application

users wrongly believe that they have sophisticated security at that particular level since their applications provide a form of role-based access control or equivalent. It should be understood that no matter what security measures are supported at the application level they are only ever going to be superficial to the knowledgeable adversary or malicious insider. This approach has a significant limitation in that the overall application system can be no more secure than the software libraries invoked and incorporated into it as well as the underlying OS upon which the applications depend through such actions as systems calls, dynamic library activation, use of intermediate code interpreters, such as “JavaScript”, or “just-in-time (JIT)” compilers, etc. The OS itself can be no more secure than the firmware and hardware facilities of the computer on which it operates. Likewise, any other software component set, such as “middleware”, DBMS, network interface structure or “stack”, is constructed above the operating system and so totally depends upon security functions provided by the operating system as well as the robustness of that operating system against attack.

	①TCP/IP Model	②OSI Model	③HIS Architecture
Software System Components	Application	Application Presentation	Healthcare applications DBMS Middleware
	(no present)	Session	Data network management system Operating system
	Transport	Transport	
	Internetwork	Network	
	Hard-ware	Network Access	Data Link Physical

Table 1: ①TCP/IP Model, ②OSI Model and ③General HIS Architecture

3.2 Open Trusted Health Informatics Scheme (OTHIS)

To achieve a high level of information assurance in HIS, our research to date has indicated that an overall trusted HIS involves the definition of structures at a number of levels in computer hardware, OS design and facilities, data network control system and health service applications. We propose a new approach to a more trusted structure, the *Open Trusted Health Informatics Structure (OTHIS)*, with the aim of addressing privacy and security requirements in a holistic manner. OTHIS defines privacy and security requirements at each level within a general HIS architecture to ensure the protection of data from both internal and external threats. It is also aimed at providing conformance of any HIS to appropriate regulatory and legal requirements in Australia. OTHIS is a broad architecture that can allow for different levels of abstraction depending upon what types of security services and mechanisms are required.

The OSI reference model (ISO 7289-1) (Table 1: ②) is well known and acknowledged as a baseline for categorisation of network communication functions and assessment. In fact, a fully operational information system based on the full seven-layer OSI model, and its associated technical standards, never attained strong market acceptance. The OSI model envisaged management and control facilities existing at each layer but many of the necessary full specifications and activities at each layer were never completed. Instead, TCP/IP (Table 1: ①) is the model normally used on a global basis for large scale structures in data network communications. The TCP/IP model does not exactly match the OSI model. The processes defined in the OSI model however are contained within the TCP/IP structures. Normally HIS designs are based around distributed network systems and, therefore, it is entirely appropriate to relate the general HIS architecture to the OSI model as well as the TCP/IP model (Table 1). Our research aims to relate and describe the roles and functions performed by each module of the OTHIS architecture and to detail how they fit into the layers of the OSI and TCP/IP models in a healthcare environment.

It should be noted that the OSI model and HIS architecture can also be divided into software and hardware component categories. From the point of view of this paper the first group, software system components, is addressed. The interpretation of the requirements for appropriate levels of data granularity security in healthcare is the basis of this paper.

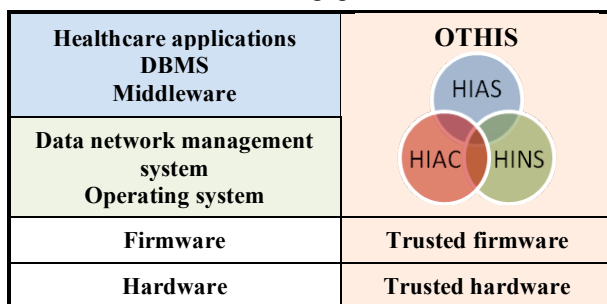


Figure 1: Open Trusted Health Informatics Scheme (OTHS)

OTHS is a modularised architecture for HIS. It can be clearly divided into separate and achievable function-based modules, like modularity in the network system structure. The advantages of the modularisation include the fact that each module is easier to manage and maintain. One module can be changed without affecting the other module. OTHIS is, thus, a broad architecture covering those requirements and parts that may be selected as required to meet particular circumstances.

Any information system depends, fundamentally, upon a trusted base for safe and reliable operation, commonly referred to as a “*trusted computing-base (TCB)*”. Without a TCB any system is subject to compromise. In particular, data security at the application level can be assured only when the healthcare application is operating on the top of the TCB platform. Otherwise the adversary can exploit illicit means to perform the actions that bypass or disable the security features of healthcare

applications or that grant inappropriate access privileges. Inevitably healthcare applications or databases must be executed the trusted platform to achieving adequate information assurance. OTHIS (Figure 1) is a broad structure that is aimed at running on top of trusted firmware and hardware bases. OTHIS consists of three distinct modules: HIAC, HINS and HIAS. There is some overlap with these three modules of the OTHIS; however, each module has a specific focus area (listed in Table 2).

OTHS Module	Focus	Information State
Health Informatics Access Control (HIAC)	Data centric	Information at rest
Health Informatics Application Security (HIAS)	Process centric	Information under processing
Health Informatics Network Security (HINS)	Transfer centric	Information under transfer

Table 2: OTHIS Modules

3.3 Health Informatics Access Control (HIAC)

3.3.1 Access Control

Access control is one of the fundamental security mechanisms used to protect computer resources, in particular in multi-user and resource-sharing computer based environments such as those incorporated into a contemporary HIS. The lack of adequate access control and associated system management in health relevant computer systems has been demonstrated on numerous occasions in recent history, including the privacy invasion situation at Australia's Centrelink (Sharanahan and Karvelas 2006), the lack of adequate safeguards in the UK NHS patient records system (Leigh and Evans 2006), and the significant IT security weaknesses identified in the US HHS information system (GAO 2006). These types of information privacy violations or weaknesses have the potential for inflicting, and do inflict, major harm on HIS consumers and providers alike. The issue of providing suitable computer OS access control in such systems is not an insurmountable one. Indeed, appropriate computer-based access control schemes do exist and can be deployed to address these information security issues.

Access control mechanisms, then, are used to define and then restrict users' access to resources. Organisations would normally use these controls to grant employees, for example, the authority to access only the information those users need to perform their duties, i.e. the principle of “least privilege”. Access controls can limit the activities that an employee can perform on data at the level of granularity desired. Access control mechanisms are therefore enabled at the OS level as well as higher levels including data network management and the database management systems for the application.

The traditional approach to access control in computer systems has been bound up with the requirements at the OS level. The 1983/1985 “*Trusted Computer System*

*Evaluation Criteria (TCSEC)*⁶ or “*Orange Book*” first brought to the attention of both the commercial ICT industry itself and to users of IT products and services, the security needs at that level. However, the level of granularity that applies at the OS level is aimed at the needs at that level for larger identified system components: data and executable program files, input/output devices, network components, software processes, threads, etc. Discretionary access control (DAC) essentially assigned responsibility for all security parameters to the “owners” (users) of such larger entities, usually their creator, who could pass on such parameters to others and perform functions as desired. Role based access control (RBAC) refined the concept to allow for users to be grouped into defined functions or “roles” allowing for far easier management of overall system security policy particularly in dynamic business environments. Mandatory access control (MAC), originally designed to meet confidentiality requirements of military systems within rigid structures, allowed systems to be created that could, in principle, enforce security policy as set out by the overall enterprise and not set up by definition provided by file/program “owners”.

The majority of current information systems are based around computer systems that implement the DAC concept. This is particularly true for commodity or “commercial-off-the-shelf (COTS)” products and systems. Examples of these computer systems include Microsoft Corporation’s “Windows” series of OS, 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, however, MAC-based systems are more appropriate to, and capable of, satisfying the specific requirements of privacy and security for information resources. Overall the MAC mechanism can, for example, provide the system with better protection from malicious or flawed applications, which can potentially damage or destroy the system and its information, and attacks from “insider” users. It can also provide higher levels of protection against an external adversary penetrating the system by exploiting “Trojan Horse” type attacks, viruses, malware, spyware, root-kits, social engineering or other illicit means to gain total access control or to tamper with audit systems.

3.3.2 Building in MAC, RBAC, DAC and others to HIAC

ICT is now sufficiently advanced that a MAC-based electronic healthcare management system is feasible. OTHIS 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

⁶ TCSEC was published by the US Department of Defense (DoD) in 1983. The written text came in book form with an orange cover, so it also became known as the “Orange Book”. In meeting a specific DoD requirement for computer systems, TCSEC was designed to prevent the leakage of confidential information by the use of a ‘security clearance’ classification system for both information structures and end users.

approach to overcoming many of the privacy and security issues which have plagued previous attempts at electronic health management systems. The HIAC model is necessarily MAC-based accompanied by RBAC administration 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.

For general applications, currently available products that support the MAC principles of a trusted OS include “*Red Hat Enterprise Linux (RHEL) Version 5*”⁷, “*Fedora Core 6*” and “*Sun Microsystems Solaris 10 with Trusted Extensions Software*”. The first two of these incorporate the results of “*Security Enhanced LINUX (SELinux)*” research originally undertaken by the USA’s National Security Agency (NSA). It should be noted that while HIS appear to use earlier DAC-based systems, modern systems (as listed above) based around such MAC oriented OS, have obtained commercial reality as well as being evaluated under the internationally accepted Common Criteria.

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 RHEL version of SELinux. These help prevent applications interfering with each other such that an unauthorised user cannot gain overall control of the system, as is possible with DAC.

In general HIAC provides for maximum flexibility within a strongly secure environment. This means achieving a balance between security needs and flexibility of implementation. This balance is primarily determined from a risk assessment related to overall privacy imperatives. For example, HIAC provides the flexibility of having an emergency override function by switching to a defined emergency policy or “profile”, in the terms used in the experimental system based on RHEL 4, in emergency circumstances. Full, enforced auditing of the system deters potential abuses of this flexibility.

To determine the practical viability of an HIAC model for HIS a demonstrator, based on an SELinux enhanced OS with MAC and RBAC approach (RHEL 4) was built (Henricksen et al. 2007). 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.

3.3.3 Granularity in the HIAC Model at the Application Level

While privacy and security requirements directly relate to identifiable data and information, a far finer level of granularity is needed for security and control

⁷ In June 2007, RHEL Version 5 operating on IBM systems is recently certified at EAL 4 Augmented for 5.3.2 LSPP, the Controlled Access Protection Profile (CAPP) and RBAC Protection Profile available at <http://niap.bahialab.com/cc-scheme/vpl/>. The LSPP conformant products should support MAC and DAC mechanisms. CAPP adopts only DAC policy.

management requirements of a real HIS. In this regard, HIAC aims at addressing access control requirements in a holistic manner, capable of defining privacy and security requirements at higher layers in an HIS according to the broad OSI model shown in Table 1 and Figure 1.

Within the HIAC structure, healthcare applications can be broadly placed into three classes. These include:

- (a) healthcare applications that totally depend upon access control parameters and their enforcement at the higher abstraction level of a computer/network operating system;
- (b) healthcare applications which provide access control definition, functionality and enforcement for an overall, enterprise-defined set of data access and program activation rules within the application programming code; and
- (c) healthcare applications which depend upon access control definition, functionality and enforcement on the database management system used to maintain necessary healthcare databases, i.e. the data accessibility at table/view level, row/column level and cell-level in databases.

The healthcare application of type (a) provides only to a certain level of granularity where it enforces access controls on files and file directories within the trusted OS level, but it does not provide access controls at table/view, row/column and cell level in the database.

The healthcare application of type (b) must be tested and evaluated against mandatory healthcare information protection requirements. This may involve analysis of detailed legal and regulatory requirements at the application designer level. Any information assurance requirements imposed upon the application must be reliably enforced. Such enforcement must be capable of a high level of trust. This type of structure can be costly and difficult to maintain without associated or complementary information assurance management applications. In many cases this means that multiple trusted application programs need to be created where appropriate levels of security functionality are entrusted to each program component.

In reducing the maintenance cost by managing security at the application level, the healthcare application of type (c) combines such structures with the finer levels of granularity needed for both data and processes relevant to the healthcare sector. In fact a number of relational database vendors, such as IBM, Oracle and Microsoft, offer access control techniques at table/view, row/column and cell level to restrict data accessibility in relational databases to a finer degree of granularity. These techniques include encryption processes at the associated levels of granularity.

The ability to achieve finer granular levels of access control at table/view, row/column and cell levels on the health records is achieved by the typical approach of adding security labelling rows to the database. A label is used to describe the sensitivity of an object or the permissions of a subject (e.g. users or processes). A subject can access an object if the subject's clearance level dominates the security level of the object. This

exemplifies the MAC policy where the overriding information access rule is based on a concept of "clearances" for users and "classification" for information, both defined by the owner of the information system and not by its users or developers. Access permissions are determined by a user's clearance compared with the sensitivity or classification level label on information stored in the system.



Patient name	Sex	...	Permanent Disability	Powers of Attorney
Vi Lee	F	...	Macular degeneration	 (encrypted)
Lu Ho	M	...	 (encrypted)	liver donation

Table 3: Example of encrypted data elements in a patient record

As illustrated in Table 2, it is possible that data may need control at a finer level than that of the entire row in a table in the database. Microsoft (Rask et al. 2005) provides a security technique by using an encryption mechanism to restrict access to any arbitrary data element at the cell-level within the database.

3.3.4 Backup and Audit Trail in the HIAC Model

Audit trails could be capable of efficient information policy assurance implementation by application of the three types of health applications within the HIAC structure as outlined in Section 3.3.3, that is security through access control delegated to the level of the trusted operating system capable of enforcing MAC profiles. The HIAC architecture enables the adoption of only those security services and methods necessary for the appropriate level of assurance in each case. In the case of an audit trail, HIAC at the OS level may be sufficient. An additional encryption method may, however, need to be invoked to protect audit trail information when in backup or transmitted form.

Backup structures could similarly depend for security functionality and enforcement on the type of healthcare applications within the HIAC structure, that is security functionality definition enforcement at a higher OS level of abstraction as for audit trails. In particular, the protection of audit trails and backup may rely on the security features and enforcement of the trusted OS to have sufficient protection.

HIAC involves a combination of all three broad structures of healthcare applications mention above. It goes further, however, in that it incorporates necessary and appropriate security mechanisms where these are required, for example the use of encryption at the table, data record and/or data element (cell) level. This research aims at a structure and method for the definition of appropriate locations for the insertion of necessary security mechanisms within an overall HIS, as envisaged in the original open systems interconnection security

architecture through standards ISO 7498-2⁸ and ISO/IEC 7498-4⁹. It should be noted that these security architecture standards (ISO 7498-2 and ISO/IEC 7498-4) identified necessary security services and mechanisms as well as their management along with the appropriate point or location of such mechanisms and services within an overall OSI architecture. This research adopts the broad architectural concepts as proposed in those standards and as adopted for some time by national governments via “*Government OSI Profiles (GOSIP)*”.

The HIAC architecture envisages that legacy systems will need to be incorporated into more modern HIS. This is allowed for by the ability of HIAC to cater for different levels of information granularity. Overall management of HIAC structure systems will require the clear design and deployment of associated security management structures. The encryption methods used, for example, require an associated cryptographic key management facility operating at whatever level of granularity is required in a particular HIS, for example at the data element, database table, file, network connection “port” level. This overall HIAC management architecture is the basis of a further research paper.

3.4 Health Informatics Application Security (HIAS)

Legislation, regulation and enterprise policy in relation to privacy and security in health informatics normally involves specific data entities (such as service provider, patient identity, etc.) rather than higher level information technology constructs. Such data entities, however, must themselves exist within those same larger constructs (e.g. databases, messaging systems, operating system file structures and the like). While privacy and security requirements directly relate to identifiable data and information, those HIS elements sitting at higher level information system layers cannot be ignored.

The overall aim of the HIAS model is to address the data protection requirements reflected in such regulatory instruments with the practical security services and mechanisms provided by healthcare application systems. In this regard, HIAS aims at defining privacy and security requirements at the application level in an HIS according to the OSI model shown in Table 1. HIAC and HINS provides the security services that HIAS needs through the authentication of claimed identities throughout HIS following by the adequate access control management. HIAS is located at the OSI’s “Application Layer”, Layer 7, to provide security features which are often required by a healthcare application at a data element level through to a service level.

⁸ ISO 7498-2:1989 Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture, functions as a discipline to identify services and mechanisms should be placed in the security architecture.

⁹ ISO/IEC ISO 7498-4:1989 Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 4: Management framework.

One of the benefits of an integrated, readily accessible, electronic health record system is that it can facilitate healthcare information exchange between healthcare providers. Healthcare providers may use different healthcare applications from multiple vendors with various information formats and, thus, the exchange of clinical information between disparate HIS can be impeded. In order to allow different HIS to effectively and securely communicate with one another, healthcare information must be sent using a consistent standard or protocol to improve compatibility and interoperability among a variety of healthcare applications and systems.

NEHTA argues WS as the most appropriate mechanism to support secure messaging between participants in the healthcare sector (NEHTA 2006). The WS technology can incorporate security features in the application layer, i.e. “WS-Security”, in the header of a “*Simple Object Access Protocol (SOAP)*”¹⁰ XML message. WS-Security provides a set of mechanisms to maintain finer granular levels of security services, such as authentication, confidentiality, integrity and non-repudiation at an element level. For example, WS-Security defines how to use XML Encryption and XML Signature processes in the SOAP to secure message exchanges (Buecker et al. 2007). Moreover, WS is a series of open standards intended to support interoperability in an environment where separate applications need to share information over an open network. This, however, provides end-to-end security for data and messages in transit but depends upon underlying processes as described above.

OTHIS must cater for the situation where WS structures are being used as the major health informatics information transport methodology. OTHIS recognises that the SOA approach, implemented through a WS structure, has become a major information architecture paradigm. As such, any healthcare security architecture must be capable of handling the WS paradigm in a trusted, secure and efficient manner.

3.4.1 HL7 and Secure Inter-application Messaging

Health Level 7 (HL7), an American National Standards Institute (ANSI) accredited standard, has been developed to enable disparate healthcare applications to exchange key sets of clinical and administrative data. With respect to the HL7 structure, HIAS depends upon the use of cryptographic subsystems as its security mechanism.

In developing a trusted system architecture for an HIS, it is important to understand the philosophy of HL7 for medical data transfer. Future research programs under OTHIS will elucidate the relationships between the broad HL7 structure and that of OTHIS from an information assurance perspective. In particular, the focus is on the use of HL7 for both communication and application security and privacy services are needed.

¹⁰ SOAP, platform independent protocol, normally uses HTTP/HTTPS as the mechanisms for exchanging XML-based messages over networks.

It is necessary to determine just what parts of the HL7 standards set belong to either of, or both, HIAC and HIAS. The problem of secure messaging structures, however, belongs to the HINS component, as described in a forthcoming paper. For example, HL7 requires the use of “digital signatures”. Reliable digital signatures are expected to be created from subsystems within the computer OS, and also possibly specific computer hardware under which the HIS works. Without a trusted foundation, the data security of any health applications must be vulnerable.

3.5 Health Informatics Network Security (HINS)

HINS consists of the appropriate network level security structure within an underlying HIS. HINS is aimed at the provision of services and mechanisms to authenticate claims of identity, to provide appropriate authorisations (least privileges) following authentication, to prevent unauthorised access to shared health data, to protect the network from attacks and to provide secure communications health data transmission over the associated data networks.

The major function of HINS is the authentication of claimed identities throughout a healthcare information system, including not only all personnel but also all computing, data storage and computer peripherals such as printers, scanners and network interfaces. Such authentication extends not only to the individual claimed identity, but to its authorised function. For example, a printer unit in a pharmacy or dispensary area in a hospital is an important component in an overall HIS since it may be used to print prescriptions from medical staff, labels for medication containers incorporating pharmaceutical identities and required dosage/usage, etc. Such an activity, for example, may be mandatorily associated with this printer element and no other. As outlined earlier, once a claimed identity has been authenticated, appropriate authorisations may be activated through HIAC components. In this sense, authorisation is separate from authentication. The OTHIS structure allows for such authorisations to be separated, identified, defined and enforced.

HINS involves the vital integration of network security protocols and associated data formats with the access control structures contained within an OS and allied generic application systems of individual computer nodes. In the generic sense this need for efficient, reliable and trusted integration is exemplified by the Cisco and Microsoft NAC/NAP¹¹ proprietary security structure. HINS has, as an overall aim, the extension of

such NAC/NAP architecture to the requirements of healthcare applications themselves, usually based upon large database management systems.

4 Conclusion and Future Work

In conclusion, the overall HIS architecture must evolve into a set of complementary security architectures which, at least, incorporates those proposed under the OTHIS scheme consisting of HIAC, HIAS and HINS. This proposed OTHIS scheme will be tested through experimental structures created on an SELinux-based computer platform. Key research questions to be answered include those concerning both system efficiency and availability aspects of the proposed architecture. This paper presents a broad architecture for high-trust HIS based around the concepts of “mandatory access control”. Preliminary results of this research indicate that the broad philosophy of MAC appears ideally suited to the protection of the healthcare information systems environment. The reasons for this may be summarised as follows:

1. Not all people and sub-systems involved in an overall system operate at the same level of security and trust.
2. People have different roles depending upon their function. Those functions depend upon factors such as qualification levels, experience and legal responsibilities.
3. The healthcare environment is rapidly moving to the use of commercial COTS systems interconnected via the global open Internet. As such, MAC philosophies are essential to safeguard the individual computer node points and thus all transmission paths for electronic health records

The aim of this research paper has been to re-examine and re-evaluate MAC philosophies in the light of (a) current requirements such as those for an HIS and (b) the current ICT product and systems environment. This research re-evaluates MAC under the OTHIS structure from the viewpoints set out above. More than two decades ago the MAC mechanism was introduced to commercial systems in order to reliably define and then restrict access to computer resources. OTHIS, while proposing underlying access control structures based around the broad principles of early MAC structures, aims at re-evaluating those MAC structures against the healthcare informatics environment and the universal usage of commodity ICT products and systems. HIAC aims at combining such structures with the higher levels of granularity needed for both data and processes relevant to the healthcare sector.

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 structures. 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

¹¹ NAC/NAP is a Microsoft and Cisco’s joint structure for Microsoft Network Access Protection (NAP) and Cisco Network Admission Control (NAC) interoperability. Microsoft NAP is a policy enforcement platform incorporate into Windows Vista and Windows Server Longhorn. Cisco NAC consists of a set of mechanisms developed into Cisco’s networking infrastructure
<http://blogs.msdn.com/windowsvistasecurity/archive/2006/09/06/742775.aspx> accessed 27/04/07.

and healthcare consumers (privacy and security), and flexible operational demands in a modern HIS.

This paper emphasises the need for well-directed research into the application of security-enhanced operating systems to provide a viable, real-world trusted HIS.

5 References

- Buecker, A., Ashley, P., Bouyssou, J., Gargaro, G., Muppidi, S., Neucom, R., Readshaw, N. and Schinke, G. (2007): *Understanding SOA Security Design and Implementation*, IBM Corp.
- HIPAA Security Series, CMS
http://www.cms.hhs.gov/EducationMaterials/04_SecurityMaterials.asp#TopOfPage. Accessed 22/05/2006.
- Information Security: Department of Health and Human Services Needs to Fully Implement Its Program, GAO
<http://www.gao.gov/new.items/d06267.pdf>. Accessed 20/11/2006.
- Graauw, M. d. (2005): Implementing Web Services in Dutch Healthcare.
http://www.ringholm.de/docs/03030_en.htm. Accessed 22/08/2007.
- Henricksen, M., Caelli, W. and Croll, P. R. (2007): Securing Grid Data Using Mandatory Access Controls. *5th Australian Symposium on Grid Computing and e-Research (AusGrid 2007)*, Ballarat Australia.
- Warning over privacy of 50m patient files (2006): Leigh, D. and Evans, R.
http://society.guardian.co.uk/health/news/0,,1936403,0_0.html. Accessed 01/11/2006.
- NEHTA (2005): Towards a Secure Messaging Environment.
www.nehta.gov.au/index.php?option=com_docman&task=doc_download&gid=63&Itemid=139 Accessed 22/08/2007.
- NEHTA (2006): Privacy Blueprint - Unique Healthcare Identifiers.
http://www.nehta.gov.au/index.php?option=com_content&task=view&id=163&Itemid=144. Accessed 19/08/2007.
- NEHTA (2006): Towards a Secure Messaging Environment
www.nehta.gov.au/index.php?option=com_docman&task=doc_download&gid=63&Itemid=139. Accessed 6/09/2007.
- Implementing Row- and Cell-Level Security in Classified Databases Using SQL Server 2005, Rask, A., Rubin, D. and Neumann, b.
<http://www.microsoft.com/technet/prodtechnol/sql/2005/multisec.mspx>. Accessed 15/08/2007.
- Welfare workers axed for spying (2006): Sharanahan, D. and Karvelas, P.
<http://www.theaustralian.news.com.au/story/0,20867,20223075-601,00.html>. Accessed 27/11/2006.