Secure Knowledge Management for Health Care Organizations

Authors: D.Mundy, D.W.Chadwick

Abstract

As the health care industry enters the era of knowledge management it must place security at the foundation of the transition. Risks are pervasive to every aspect of information and knowledge management. Without secure practices that seek to avoid or mitigate the effects of these risks, how can health care organisations ensure that knowledge is captured, stored, distributed, used, destroyed and restored securely? In an age where risks and security threats are ever-increasing, secure knowledge management is an essential business practice.

The cost of security breaches in a health care context can range from the unauthorized access of confidential information to the potential loss or unauthorized modification of patient information leading to patient injury. In this chapter the authors highlight different approaches to minimising these risks, based on the concepts of authentication, authorization, data integrity, availability and confidentiality.

Keywords: Authentication, Authorization, Privacy, Encryption, Digital Signature

1 The Context For Secure Knowledge Management

Knowledge is intangible, expensive to obtain, easy to lose and invaluable to organizational success. An organization’s knowledge can also be easy to view, steal, manipulate and delete. In the physical world knowledge is protected by structures such as non-disclosure agreements, filing cabinets and shredding machines. In the digital world the same kind of mechanisms are required to ensure our knowledge is well protected.

Security threats to organizational data are increasing exponentially both within organizational boundaries and externally. According to the respected CSI/FBI Computer Crime and Security Survey 2002 [Power, 2002] the largest majority of attacks on computer networks are internal. In this chapter initially we present a conceptual model for ensuring secure knowledge management in health care. Then we introduce key security technologies which can be used to implement components of the model, as well as providing background information on how these components have traditionally been implemented within IT systems. Finally we provide case studies of recent implementations that illustrate use of the model. We believe this will convince the reader that security is a necessity in the implementation of Knowledge Management Systems (KMS).

2 Ensuring Secure Knowledge Management in Health Care

A model for ensuring secure knowledge management in health care is shown in Figure 1.

?? ***authentication:*** ***1.*** *Security measure designed to establish the validity of a transmission, message, or originator,* ***2.*** *a means of verifying an individual's eligibility to receive specific categories of information.* [NIS, 1992] (see section 3)

?? ***authorization:*** ***1.*** *The rights granted to a user to access, read, modify, insert, or delete certain data, or to execute certain programs.* ***2.*** *Access rights granted to a user, program, or process.* [NIS, 1992] (see section 4)

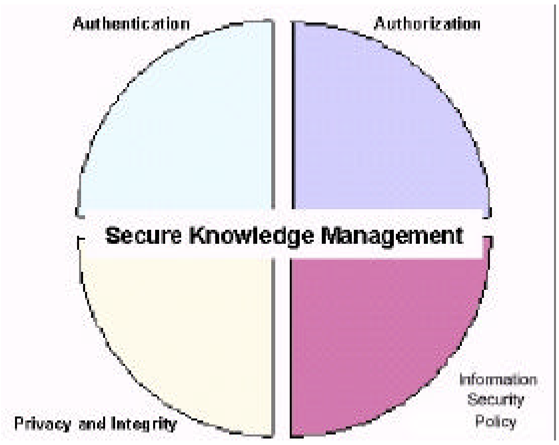
?? ***data security (privacy):*** *[The] protection of data from unauthorized (accidental or intentional) modification, destruction, or disclosure.* [NIS, 1992]*;*

?? ***data integrity: 1.*** *[The] condition that exists when data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed.* [NIS, 1992] (See section 5)

?? ***information security policy:*** *organizational guidelines, rules, regulations and procedures that are used to protect an organisation's information* (see section 6)

Each of the four components are essential and mutually supportive. Authentication without authorization would mean that only valid users could gain access, but could execute any operations they wish to within the KMS. For example, in a patient records system secretaries (who might be authorised to update a patient's name and address only) could execute a command to access health details for all patients or change diagnoses. Conversely, authorisation without authentication would mean that anyone could masquerade as anyone else and thus gain his or her access rights. Information security policy provides the risk management, the appropriate controls, the recovery procedures, and the auditing procedures etc. Without an information security policy there would be no apparent requirement for secure practices, and security would either be ignored or implemented in an ad-hoc manner, with the result that some controls could be too rigid and others completely missing. Finally, a system without privacy and integrity would be untrustworthy, so the knowledge contained within the system would be virtually worthless. For example, in a knowledge base containing details about clinical procedures, erroneous changes could be made to the information without detection, possibly leading to fatal consequences for patients.   This model will be examined in greater depth in the next few sections, which provide information about mechanisms for implementing each segment of the model. Following these sections case material will be provided demonstrating the model in action.

Figure 1 Model for Secure Knowledge Management



3 Authentication Mechanisms

3.1 Authentication

How can you be sure that the user requesting access to your KMS is who they say they are? Traditionally, weak authentication systems, typically based on a username and/or password, have been a key source of unauthorised access to networks and computer systems. From a health care KMS perspective, authentication mechanisms provide a means to ensure that external parties that we don't wish to access the KMS cannot gain access without acquiring an authentication token. If we choose a strong authentication mechanism then it should make it extremely difficult, if not impossible, for these parties to gain access to our KMS. Particular risks of poor authentication in health care would include potential unauthorised access to a KMS containing information, for example, on patient conditions, quality of patient care or hospital procedures. All attacks potentially could result in decreased patient care and liability or negligence cases.

In the USA and other countries, government regulations such as the Health Insurance Portability and Accountability Act (HIPAA) mandating the privacy of patient identifiable information, require that access only be granted to those parties authorised to view the information. Strong authentication of users seeking access to a KMS containing patient related material will be essential in achieving compliance with these kinds of regulation.

3.2 Present Practices – Passwords and Their Frailties

Traditionally, authentication to networks and computer systems has been provided by the use of usernames and passwords. In early password authentication schemes users would simply log on using their username and password and the computer system would do a simple lookup that the password given matched the password stored for the user. However, password files could frequently be obtained from the system itself and then posted for all to see. So developers were required to secure the scheme by taking the password and passing it through a programming routine called a one time hashing algorithm. The hashing algorithm mathematically reduces the data into a small (typically 128 or 160 bits), indecipherable series of bits. The hashed password can then be stored in the system instead of the clear text password. When the user logs into the system the password they input is hashed and the new hash and the stored hash are compared to see if they match.

Password hashing is now commonplace but hashed passwords are still vulnerable to dictionary attacks. This is where the attacker runs all the words in a dictionary through the hashing algorithm, and compares the generated hashes with the stored hashed values. Bad as this might seem, a potentially far greater threat than poorly protected password storage, is the threat of human weaknesses. Users are prone to picking poor passwords, writing passwords down, and giving their passwords out etc. Management steps should be taken to educate users and strengthen password usage. Simple information security policy statements such as passwords must be eight characters or more in length and must contain a mixture of capital letters, lowercase letters and digits, provide improvements to the basic system and usually render the passwords impervious to dictionary attacks. User education can also lead to a movement away from bad habits such as leaving passwords on post-it stickers and giving passwords out to other people.

However, even with the various protection mechanisms mentioned above, passwords are still relatively weak. To be effective they rely on secrecy and strict policy management. In Health environments where perhaps access to PC's is not strictly controlled, especially on wards where patients or other parties could gain unauthorised access to the PC, passwords are not an effective authentication mechanism. To gain effective authentication other mechanisms can be used both in conjunction with and as replacements for passwords.

3.3 Key Technology Focus – Biometrics

Biometrics allow users to authenticate themselves using personal characteristics that are less easily stolen or copied. On a user there are certain uniquely identifying attributes that can be used to determine identity e.g. fingerprints, retinal scans, facial imaging, voice recognition, hand readers etc. Biometric authentication comprises three phases. Firstly a template of the user’s biometric feature is recorded by the system. A biometric device reads the user’s biometric feature several times and stores the average of the readings in the system. Several readings are needed because biometrics vary according to temperature, humidity, blood pressure etc. Then when the user wishes to authenticate to the system, a biometric device records the user’s biometric feature (phase two), finally the reading is compared with the stored template using some pre-defined matching algorithm (phase three). Unfortunately, due to the imprecise nature of the matching, biometric authentication is prone to false positives and false negatives. False positives are when an attacker is wrongly identified as being the user, and false negatives are when the user is not recognised by the system.

Biometrics technology has been piloted in a number of organizations (e.g. Essex Police and Securicor (UK), Washington Hospital Centre (DC)) and full-scale implementations are already in place in a number of business sectors (e.g. Nigerian electoral process, and the City of Glendale (CA)). In future KMS, biometric authentication will increasingly become the authentication mechanism of choice.

3.4 Key Technology Focus –Public Key Cryptography, Public Key Infrastructure (PKI) and Digital Signatures

The concept of Public Key Cryptography was introduced to the academic community in 1976 by two researchers called Whitfield Diffie and Martin Hellman [Diffie and Hellman, 1976]. Public Key Cryptography was initially applied to encryption (covered in section 5.2, basically encryption means to disguise data and decryption means to retrieve the data that was previously disguised) but it also solved the problem of authentication. The basic idea of Public Key Cryptography is to have two different security tokens, called the *public* and *private* keys, which work together as a pair. They can be used to perform mathematical operations on data, either digital signing/verification or data encryption/decryption. The *public key* is viewable to all users whilst the *private key* remains a secret to the entity to whom the keys have been given. If data is encrypted with the *private key*, it can only be decrypted with the *public key*, and vice versa. It is not possible to both encrypt and decrypt the data with the same key, nor is it usually possible to determine one key from the other. When data is encrypted with the *private key* of a user, this allows the data to be authenticated as coming from that user. When data is encrypted with the *public key* of a user, this allows the data to be made confidential for that user.

However, public key cryptography is slower to execute than conventional cryptography, which uses a single key. For this reason, when data authentication is required, the data is first condensed using a hashing algorithm. The hash value is called a *message digest*. The *private key* of the user is then used to encrypt the *message digest*. The encrypted digest is known as the *digital signature* of the data. The *digital signature*, along with the original data, are then sent to the recipient. On receipt the receiver takes the *digital signature* and decrypts it using the signer’s *public key*, to reveal the message digest created by the signer. The recipient then creates his own message digest from the data sent by the signer and compares the two. If the two *message digests* match then the recipient can be sure that the data was sent by the signer and it has not been changed on route.

However, this pre-supposes that the recipient is in possession of the genuine public key of the signer. Whilst it would be possible for all users to personally meet and exchange their public keys with each other, this is not a scalable solution. Consequently we need a reliable and trustworthy way of distributing public keys. A trusted third party, called a Certification Authority (CA), is used to digitally sign the public keys of users, to ensure that they cannot be tampered with. A CA would be contained within and managed by a hierarchical authority, for example the Department of Health and Human Services or a hospital's Human Resources department. The CA signs a message containing the name of the user and their public key, and its own name, and these certified public key messages are called Public Key Certificates (PKCs).

Should a user's private key become compromised e.g. stolen, then we have a requirement to communicate this knowledge to other users. This is generally done using a particular construct called a Certificate Revocation List (CRL). A CRL contains a list of all the public key certificates no longer considered to be valid because the private key has been compromised or revoked, and the CRL is signed and dated by the CA.

A Public Key Infrastructure is seen as '*the set of hardware, software, people, policies and procedures needed to create, manage, store, distribute, and revoke PKCs based on public-key cryptography*' [Arsenault and Taylor, 2002]. Recently mechanisms for digitally signing the popular eXtensible Markup Language (XML) documents have been introduced [Eastlake et al., 2002]. Within a health care KMS users would generate XML documents, the content of these documents would then be digitally signed with the user's private key. When any user wishes to retrieve the document they can then check the verification of the XML Signature using the public key of the signing user.

3.5 Key Technology Focus – Smartcards

Modern smart cards contain a computer embedded chip and user specific data, which can be used to provide authentication when placed in a smart card reading device. The user specific data can be anything linked to the user, such as a private key or a digital fingerprint. Traditionally this user specific data would have been stored as a software token on a PC, making it liable to theft or deletion. Smart cards provide increased security because the user specific data is never allowed to leave the smart card. All processing operations are carried out via the on-board chip so the user specific data can never be copied. Usually the data is further protected via the use of a password.

Previously high costs and unreliability [Chadwick, 1999] have been a significant factor in the slow adoption of smart card technology. Costs have significantly decreased recently, and reliability has improved, so the adoption of smart cards becomes a viable option to the other authentication alternatives.

4 Authorization Mechanisms

4.1 Authorization

Authorization provides assurance that the users accessing the KMS have permission to do so. When authorization is combined with a suitable authentication scheme we can be sure that the users accessing the system are who they say they are and are authorized to access the resource. Different access control models have been developed to ensure that only authorized users can access resources. From a health care KMS perspective, we wish to ensure that users are, for example: authorized to access the system, authorized to generate new knowledge within the system, authorized to make changes within the system.

4.2 Discretionary Access Control (DAC)

Discretionary Access Control (DAC) can be viewed as owner based administration of access rights. In DAC the owner of an object has discretionary authority over which other users can access the object. For example Alex has just set up his own KMS and he grants access to Kate and Lee but denies access to Spencer. There are various types of DAC including a strict DAC where Kate and Lee would not be able to grant access to other users, and a liberal DAC where delegation is allowed either with a strict limitation on the number of delegation levels or with no restriction (i.e. Kate could grant to Sophie who could grant to Johnny etc…). The DAC approach has some limitations, the most notable being how the owner can delegate his discretionary power to other people.

4.3 Mandatory Access Control (MAC)

Mandatory Access Control (MAC) can be thought of in terms of security labels given to objects and users. Each object is given a label called a security classification and each user is given a label called a security clearance, which includes a classification list. This list identifies which type of classified object a user has access to. A typical hierarchical classification scheme used by the military is *unmarked*, *unclassified*, *restricted*, *confidential*, *secret*, and *top secret*. A MAC policy using such a hierarchical scheme would typically be “read down and write up”, which would help stop information leakage. A user with clearance of *restricted* could read from objects with classifications of *unmarked* to *restricted* but only write to classifications of *restricted* to *top secret*. The same user could log in as unmarked to enable them to write to levels up to *restricted*.

4.4 Role Based Access Control (RBAC)

In the basic Role Based Access Control (RBAC) model, permissions are granted to roles, then these roles are assigned to users who therefore acquire the roles’ access permissions. Roles typically represent organisational roles such as secretary, consultant etc. Roles confer both access rights to resources and the right to assign roles to users. For example, a physician may have read access to a KMS but not have the access right to alter data within it; a KMS security officer may have the right to assign people to roles but no access rights to the resources itself. A role and its permissions tend to change infrequently over time whereas the users associated with the role will change more regularly. This basic premise makes associating permissions with roles easier than associating permissions with users. Users can change roles and new users can be allocated roles. As needs change, roles can be granted new permissions or permissions can be removed. The main advantages of RBAC are in maintenance and scalability.

4.5 Key Technology Focus – Privilege Management Infrastructure (PMI)

The Privilege Management Infrastructure is a new development in the world of authorization. A PMI is to authorization what a PKI is to authentication. In a PMI a user is allocated digitally signed privileges, called attribute certificates, and these attribute certificates can be presented to a resource in order to gain access to it. The resource is governed by an authorization policy that says which privileges users must have in order to gain access, and under which conditions.

Attribute certificates are allocated to users by attribute authorities (analogous to certification authorities in a PKI). They are digitally signed by the attribute authority, and because of this they can be stored in a public repository or held by the user on their PC. In order to gain access to a resource, the user must first be authenticated by the resource to prove that he has the right to assert the privileges contained within his attribute certificates. This authentication could be by any means, e.g. Kerberos, or a digital signature and Public Key Certificate. After successful authentication the attribute certificates containing the user's privileges are verified and checked against the authorization policy. If the policy states that the privileges are sufficient then the user is granted access, else access is denied. A number of different PMI solutions are available including PERMIS and AKENTI.

5 Data Security and Integrity during Transfer

5.1 Data Security and Integrity

A health care KMS without data security and data integrity should be thought of as being untrustworthy. The information held within the system could have been altered, modified or had key sections removed. Even more importantly a KMS without data security may have leaked sensitive information to unauthorized parties. One of the key stages at which information leakage can occur is during data transfer over the network, Intranet or Internet. From a health care KMS perspective, looking at regulations such as HIPAA, poorly configured data security could result in unauthorised users gaining access to patient information and non-compliance. Without data integrity, staff will not be able to use a health care KMS effectively, as the information it provides will be unreliable.

5.2 Key Technology Focus – Data Encryption

In data encryption understandable data (*plain text)* is transformed using an *encryption algorithm* into incomprehensible data (*cipher text*) under control of a *key*. When the previous *plain text* is required the *encryption algorithm*, the *key* and the *cipher text* are used in conjunction to retrieve it. The *cipher text* looks like a random bit stream and there is no way of establishing the *plain text* from the *cipher text* without the *key*. The *key* is usually a randomly generated bit string consisting of 64-256 bits (the longer the key, the stronger the encryption). Various *symmetric encryption algorithms* exist with the most popular being CAST [Adams, 1997], RC2 [Rivest, 1998] and Triple DES [ANSI, 1985].

Encryption provides protection of the information within a KMS from unauthorized viewing as long as the text is *cipher text* and the attacker does not have access to the *key*. There are two forms of encryption that can be used, single key (*symmetric*) or dual key (*asymmetric* or *public key*). In single key encryption both parties use the same key for encryption and decryption. Dual key encryption follows the same principles described in the Public Key Infrastructure section above. Therefore encryption comes with the disadvantages of key management (who should generate keys, how to distribute keys, what to do if keys are lost) and a decrease in system performance due to the encryption/decryption process. Also encryption does not actually provide any assurance that the data has not been altered in transit and only some assurance that the data came from the person it is stated to have come from.

5.3 Secure Data Transfer Technologies e.g. Secure Sockets Layer (SSL)

SSL is a security protocol, which can be used to provide a secure channel between two machines (server and client) across an insecure network such as the Internet. The protocol has provisions for the protection of data in transit, using Message Authentication Codes (MACs) [Krawczyk, 1997], and strong authentication of the server using X.509 public key certificates. It can also provide authentication of the client and encryption of the data whilst in transit. An SSL connection consists of two phases; the handshake and data transfer phases. The handshake phase authenticates the server and optionally the client, and also establishes the shared secret that will subsequently be used in the MACs and optional encryption mechanism that will be used to protect the data. Once the handshake phase is completed the data is split up and transmitted in protected packets.

There are a large number of SSL implementations available, ranging from the free and high quality Open SLL implementation (www.openssl.org) to vendor toolkits from organisation such as RSA (www.rsasecurity.com) and IAIK (www.iaik.at). Other mechanisms exist which provide secure data transfer including Transport Layer Security (TLS) [Dierks and Allen, 1999], which is essentially an improved version of SSL, S/Mime [Dusse et al., 1998] to secure email transactions and Secure Shell (SSH) [Ylonen et al., 2000] often used for configuration management. In a health care KMS, SSL would be used to provide a protected channel for users to access information from the KMS.

5.4 Key Technology Focus – Firewalls

A firewall is a system designed to prevent unauthorised access to and from your private network. The firewall consists of a number of components:

?? The Internet Use security policy for the organization. This stipulates at an organizational level the expected security required when connecting to the Internet. (For example, all external access must be through a strong authentication system)

?? The mapping of the policy onto designs and procedures to be observed when connecting to the Internet. (For example SSL client authentication may be required.)

?? The firewall hardware and/or software used to protect the network

Each of the components is required. Without a policy the firewall can not be correctly configured, as the technical staff will not know which traffic to let in and which to exclude. Without enforcing the procedures then many aspects of the policy may simply be ignored, such as inspecting the logs on a daily basis. Firewalls can be complex a couple of the techniques used are shown below.

?? Packet Filtering - Filters network data packets based on their Internet Protocol (IP) and UDP / TCP source and destination addresses.

?? Stateful Packet Inspection - Inspects data packets as they are arriving and filters on a specific set of security rules.

Firewalls help prevent attacks against insecure services, can secure external access to required network services and provide a cost advantage over securing each host on an organizational network. However, firewalls are not without their disadvantages. Like any computer system without regular updates/patches intruders can gain access to the health care network. They may also make it difficult for legitimate users to be able to access required network services. Hackers can also often circumvent firewalls by using ‘backdoors’ into the health care network, provided for example by modems situated behind the firewall. However, the biggest disadvantage of firewalls is they provide no protection against the internal hacker. Given that hospitals are public places, this can pose a serious problem. By placing a second firewall directly in front of the health care KMS server, this can ensure that requests to that server are authenticated, and only passed through on certain ports, thereby restricting the attacker’s options.

5.5 Key Technology Focus – Wireless Data Transfer

Wireless technology, based on the IEEE 802.11 standard, is increasingly being adopted, especially in areas such as health care where the benefits of mobility are great. Unfortunately 802.11 offers only a basic level of security (open or shared-key authentication and static wired equivalent privacy (WEP) keys), but worse still, many wireless LANs are installed with no security at all or are left in default out-of-the-box configurations, thus allowing all comers to gain access to the network. Wireless LANs should always be configured with 128-bit WEP as a minimum, but even this can be compromised by the determined hacker, so wireless technology should not be used for mission critical KM applications unless the basic security is enhanced with technologies such as TLS, VPNs, IPSEC or 802.1X/EAP.

Wireless Access Points are used to set up wireless networks and connect the wireless network to the physical hard-wired network. We can compare a Wireless Access Point directly to an internal modem on the organizational network (i.e. it is a 'backdoor'). The addition of wireless to the health care network must not come at the cost of reduced security. Therefore we must think about the key elements in securing this new technology.

?? access and authentication – Open authentication involves configuring the correct service set ID (SSID) into the client. This is no more than a shared password, which, without WEP, is transferred in the clear over the airwaves, so anyone with a wireless receiver can capture it and thus gain access. By using WEP (see below), the SSID is encrypted prior to transfer, thus making it difficult for hackers to decipher the SSID. Shared-key authentication on the other hand simply uses the shared WEP key for authentication. The access point sends the client a challenge and the client must then encrypt this with the shared key and return it to the access point to gain access.

?? data privacy (Provided by using WEP encryption and shared symmetric keys)

?? network location and access point security (Physically placing the Wireless Access Point outside the health care organisations firewall may limit any damage)

Notwithstanding the security concerns above, the benefits of using wireless technology within KMSs are numerous. Specialists can record procedures in places where there might be limited 'wired' access, and doctors can be permanently online whilst doing their ward rounds.

6 Security Policy

6.1 Secure Data Management - Storage, Backup and Disposal

An information security policy is the key to secure data management. Without policies in place governing the storage, backup and disposal of information, no attention will be given to the procedures that need to be in place to enforce the policy. A security system is only as strong as its weakest link and the actual computer/storage device on which a KMS is situated can be an easy target if the attacker can gain physical access to it. Therefore in circumstances where a machine stores confidential information or business critical information its physical security must be assured. Access restrictions to the room holding the machine must be in place and strictly enforced. Furthermore, the machine itself must be protected by secure authentication and authorization mechanisms.

Backup tapes must be treated with the same amount of physical security as the systems they are used to restore. This is because the information stored within your KMS is also stored on the backup medium. If a backup medium is stolen then it is reasonable to expect that your system has been compromised. Thus backup media should be physically secured by either storing in a locked room or safe. In addition to physical security, the backup medium may also be logically protected either by using data encryption and/or an authentication mechanism to activate the restore process.

Secure disposal of storage media also needs to be an information security policy requirement. There have been instances where confidential data has been left on computers that have been passed on to other organizations. Even worse, computers can be left still set up to access your network or KMS. Simply deleting information on computers is not enough to erase the data from the hard drive. The data either has to be securely deleted using a commercial “secure delete” application, or the media destroyed. Without secure deletion procedures the health care organization and its systems are not only at potential risk from release of confidential information but also at risk from backdoors into the system.

6.2 Key Business Focus - Business Continuity Planning/Disaster Recovery

KMSs are invaluable resources. Losing the knowledge stored within such systems would invariably affect patient care and business continuation. In extreme cases the loss of an IT system can lead to the liquidation of an organisation. In the health community the loss of such a system could have results such as inefficient patient service, inaccurate diagnosis and loss of specialist practices. In extreme cases it could lead to the loss of human life e.g. if important patient records are lost and diagnoses are lost or inappropriate drugs are prescribed.

The first step in the contingency process is to look at the business impact of losing the particular KMS combined with a risk and threat analysis. This will help to highlight areas of significant risk, which will need to be covered in detail by the contingency plan or mitigated by another measure. An analysis of the risks and threats facing the KMS will lead us in the second step to the development of a comprehensive contingency and recovery plan, plus risk mitigating actions. The recovery plan will highlight procedures for ensuring business continuity should any of the risks and threats be realised. The third step will be to test out the recovery plan. A recovery plan, which does not work, is of little use in an emergency. If backup links and servers have been installed, then time needs to be set aside to test that an operational service can be brought back into use with them. If a third party backup service provider is being used, they will usually allow you time each year to test that their system can run an operational service for you.

The final step in the contingency process is the continual audit, review and update of the contingency plan and risk mitigating actions over the lifetime of the KMS. In other words, this is a continual process that never ends, so as to ensure that the recovery plan remains up to date and workable. Further, new risks are continually arising, and these have to be taken into account and new mitigating actions devised. It is essential to ensure that key personnel know the recovery plan or know where to obtain it. If for example a change has been made in IT personnel between the last audit and the new one then the audit would record if the new personnel knew about the contingency plan.

7 Case Study – PMI Implementation (Authorization Segment of Model)

In this section we present an example of how a PMI implementation can be used to provide strong authorization in our recently developed Electronic Prescription Processing (EPP) Application Programming Interface (API). In the EPP API we have integrated the PERMIS PMI API [Chadwick and Otenko, 2002] so as to control who is authorised to execute commands such as prescribe and dispense prescriptions, and also to ascertain patients rights to exemption from charges [Chadwick and Mundy, 2003]. In a KMS one could envisage using PERMIS to control rights to access the system, modify the data etc.

The overseer of the UK National Health Service, which to all intents and purposes is the Secretary of State for Health in the UK Government, would generate and electronically sign a PERMIS policy stipulating who can carry out which actions in the Prescription

Processing System. For example the policy might state that the General Medical Council is trusted to allocate the role of Doctor to qualified Doctors, and that anyone with the role of Doctor is allowed to prescribe. Therefore a signatory member of the General Medical Council indirectly gives all General Practitioners in the UK NHS the right to prescribe when they are issued with a Doctor role privilege certificate. When the GP is generating a prescription their prescription program will use the EPP API, and the latter will call the PERMIS decision engine to determine if the GP is authorised to prescribe according to the rules laid down in the policy. As long as the prescriber has the role of Doctor, they will have been granted permission to prescribe and they will be allowed access to the operation to generate an electronic prescription. Similar mechanisms exist for dispensers within the prescription processing system and for determining the exemption qualification of patients.

In a KMS we could reasonably expect the system administrator or systems manager to be the policy owner. The system manager could define roles such as reader, editor, administrator, and grant appropriate permissions to each of the roles. Each of the staff would be allocated one or more role attribute certificates according to their job functions. If for example an editor wished to modify information in the KMS then they would request access, the PERMIS decision engine would be consulted, their role attribute certificates would be retrieved and access granted or denied according to the policy.

8 Case Study – Secure Distribution of Patient Diabetes Information

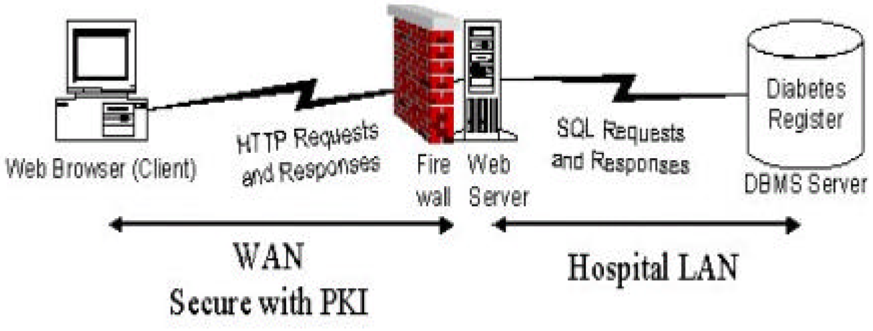
Hospitals in the UK keep a large number of patient information databases recording information about patients with chronic diseases, for both research purposes and clinical health purposes. Most of the information is only available internally to the secondary carers, and no access is provided to other health care professionals who may also be involved in the patient's care. The sharing of information between primary and secondary carers will provide a more efficient disease control system and enhanced patient care through a combination of a reduction in the number of duplicate investigations, more accurate information being available to all, and a speeding up of the business processes.

As an example of secure knowledge management, we ran a project to provide primary health care professionals with secure Internet access to a hospital Diabetes Information System (DIS). The DIS was implemented in 1992 and provides a complete record of all registered diabetic patients in the local hospital area.

The DIS is situated on the secure hospital Intranet and to provide Internet access to the system we required a strong security infrastructure (Figure 3). This is because the Internet is a highly insecure network and not suitable for the transfer of unprotected patient confidential information. The backbone behind our secure solution was a Public Key Infrastructure (PKI). The PKI provides the required pre-requisites of strong authentication and data privacy through the use of strong encryption from accessing the hospitals internal trusted network.

Requests for patient data are transmitted from the primary carer's PC via the HyperText

Figure 3 – Distributed Diabetes Information System Security Infrastructure



Transmission Protocol (HTTP) using a standard web browser. The HTTP requests are encrypted and digitally signed prior to transmission, using PKI software installed on the user’s PC, thus forming a private channel to the hospital firewall from the PC. The messages are decrypted and the digital signatures checked on the firewall, and then transferred to a web server on the hospital Local Area Network (LAN). Scripts on the web server convert the HTTP requests into Structured Query Language (SQL) requests for information from the DIS. The DIS processes the requests and sends SQL responses back to the web server. The patient information is then routed back to the client PC and displayed as web pages in HyperText Markup Language (HTML) format. All information transferred over the private channel is encrypted and digitally signed using either the users private signing key (for requests) or the hospital’s private signing key (for responses). If the user’s digital signature is successfully authenticated they are allowed access through the firewall and to the DIS. If the hospital’s digital signature is successfully authenticated the patient information is displayed (otherwise it is discarded).

This example shows that secure distribution of knowledge is possible across the Internet, using new security mechanisms with legacy databases. A full description of this is provided in [Young et al., 2001]. Looking at how the segments of our model for secure KMS have been filled in this example; we have used PKI services to secure the channel between the client and the server thereby protecting the privacy and integrity of the transaction. Authentication is provided by means of the user’s digital signature. Authorization is provided through ACL’s within the DIS. Security policy is in place at the hospital with strict rules for who can gain access through the firewall, and who can access patient data. A firewall is positioned in front of the hospital network to prevent undesirable users

9 Summary

This chapter has provided an introduction to the wide range of different security techniques that can be used to secure knowledge management applications, none of which on their own can be seen as a panacea to all of your security requirements. Simply put, a combination of authentication, authorization, privacy, transmission security and good information security policies and practices are needed to help to ensure a more secure knowledge management environment.

Returning to our model we have demonstrated through the case studies, that if each of the segments are covered, then we can be reasonably sure of the strength of our systems security. We believe the implementation of PKI or the use of third party certification services will become widespread, not only in health care environments but also in the general business world. PKI services for authentication, data security and integrity coupled with PMI for authorisation and firewalls for restricted access, all underpinned by an enforceable information security policy and procedures, combine together to provide a sound basis for secure KMSs.

10 References

[Adams, 1997] Adams, C, The CAST-128 Encryption Algorithm, *RFC2144*

[ANSI, 1985] ANSI, American National Standard for Financial Institution Key Management (wholesale), *ANSI X9.17*

[Arsenault and Turner, 2002] Arsenault, A, Turner,S, Internet X.509 Public Key Infrastructure: Roadmap, *PKIX Working Group Internet Draft*

[Chadwick and Mundy, 2003] Chadwick, D.W. and Mundy, D.P., Policy Based Electronic Transmission of Prescriptions, *IEEE 4th International Workshop on Policies for Distributed Systems and Networks*, Como, Italy

[Chadwick and Otenko, 2002] Chadwick, D. W, Otenko, A. , The PERMIS X.509 Role Based Privilege Management Infrastructure, *7th ACM Symposium On Access Control Models And Technologies*, 135-140.

[Chadwick, 1999] Chadwick, D.W., Smart Cards aren't always the Smart Choice, *IEEE Computer, 32, 12,* 142-143

[Dierks and Allen, 1999] Dierks, T, Allen, C, The TLS Protocol Version 1.0, *RFC2246*

[Diffie and Hellman, 1976] Diffie, W, Hellman, M.E., New directions in cryptography, *IEEE Transactions on Information Theory, 22, 6,* 644-654

[Dusse et al., 1998] Dusse, S, Hoffmann, P, Ramsdell, B, Lundblade,L, Repka, L, S/Mime Version 2 Message Specification, *RFC2311*

[Power, 2002] R.Power. *2002 CSI/FBI Computer Crime and Security Survey, Computer Security Issues and Trends, Computer Security Institute. VIII, 1.*

[Krawczyk, 1997] Krawczyk, H, Bellare, M, Canetti, HMAC: Keyed-Hashing for Message Authentication, *RFC2104*

[NIS, 1992] NIS, National Information Systems Security Glossary, *NSTISSI, 4009*.

[Rivest, 1998] Rivest, R, A Description of the RC2(r) Encryption Algorithm, *RFC2268*.

[Eastlake et al., 2002] Eastlake 3rd, D, Reagle, D, Solo, D, (Extensible Markup Language) XML-Signature Syntax and Processing, *RFC 3275*

[Ylonen et al., 2000] Ylonen, T, Kivinen, T, Saarinen, M, Rinne, T, Lehtinen, S, SSH Transport Layer Security, *SECSH Working Group Internet Draft*

[Young et al., 2001] A.J. Young, D.W.Chadwick, J. New. Providing secure remote access to legacy applications, *IEE Computing and Control Engineering Journal, 12, 4,* 148-156.