Methods of responding to healthcare security incidents

Steven Furnell[a], Dimitris Gritzalis[b], Sokratis Katsikas[c], Konstantinos Mavroudakis[c], Peter Sanders[a], Matthew Warren[d]

[a]Network Research Group, School of Electronic, Communication and Electrical Engineering, University of Plymouth, Plymouth, United Kingdom (stevef@pbs.plym.ac.uk; peter.sanders1@virgin.net)
[b]Athens University of Economics and Business, Department of Informatics, 76 Patission St., Athens 10434, Greece (dgrit@aegean.gr)
[c]University of the Aegean, Department of Mathematics, Karlovassi 83200, Greece (ska@aegean.gr; kmav@aegean.gr)
[d]Business Security Group, Plymouth Business School, University of Plymouth, Plymouth, United Kingdom (m.warren@pbs.plym.ac.uk)

Abstract

This paper considers the increasing requirement for security in healthcare IT systems and, in particular, identifies the need for appropriate means by which healthcare establishments (HCEs) may respond to incidents.

The main discussion focuses upon two significant initiatives that have been established in order to improve understanding and awareness of healthcare security issues. The first is the establishment of a dedicated Incident Reporting Scheme (IRS) for HCEs, enabling the level and types of security incidents faced within the healthcare community to be monitored and advice appropriately targeted. The second aspect presents a description of healthcare security World Wide Web service, which provides a comprehensive source of advice and guidance for establishments when trying to address and prevent IT security breaches.

The discussion is based upon work that is currently being undertaken with the ISHTAR (Implementing Secure Healthcare Telematics Applications in Europe) project, as part of the Telematics Applications for Health programme of the European Commission.

Keywords:

Healthcare Security; Incident Reporting; Security Guidelines; Awareness

Introduction

It is now widely recognised that Information Technology (IT) systems fulfil a vital role in the operation and running of modern healthcare establishments (HCEs). Systems are utilised in a variety of direct care and supporting activities, such that staff are increasingly dependent upon them in performing their day-to-day activities. In addition, individual systems frequently form part of an interconnected network, with the resulting infrastructure handling an increasing variety of data (of varying types and levels of sensitivity).

Whilst such arrangements deliver a number of advantages and new capabilities to healthcare providers, they also introduce additional vulnerabilities within the establishment, increasing the possibility of security breaches. As such, the need to preserve data security (in terms of confidentiality, integrity, availability and accountability) assumes ever increasing importance.

Evidence suggests that the healthcare community can be particularly vulnerable to security incidents. For example, a survey of computer abuse conducted by the UK Audit Commission in 1994 [1] showed the healthcare field to be amongst the most significantly affected (other areas surveyed included local government, education, finance, manufacturing, retail, IT and communications). The number of healthcare security incidents reported (i.e. 127 cases) was more than for any other sector save local government (with 193 incidents), and represented 24% of the total incidents reported. Furthermore, of the 334 establishments that responded, more than a third (35%) reported some kind of incident.

As a consequence of observations such as those above, the issue of healthcare security has been targeted by a number of initiatives. One such example is the ISHTAR (Implementing Secure Healthcare Telematics Applications in Europe) project, with funding from the European Commission. The objective of ISHTAR is to support healthcare security through a range of awareness and advisory activities. These include :

- creation of an advisory panel of legal, medical and technical experts on data protection;
- the establishment of a range of security training courses;
- provision of consultancy services to other healthcare projects;
- establishment of a healthcare-specific incident reporting scheme (HIRS);
- creation of a security dissemination service based on the World Wide Web (WWW).

The latter two aspects constitute the main focus of this paper and can be seen to offer complementary services. The HIRS provides a means for HCEs to report (and be notified of) incidents affecting them in practice, whilst the WWW service offers the means to disseminate wide-ranging advice which HCEs may consult as and when required (including when faced with the need to respond to an incident). The paper will now present these areas in more detail, describing the overall concepts and the main achievements to date.

Healthcare Incident Reporting Scheme

An Incident Reporting Scheme (IRS) is an information system responsible for gathering, evaluating and processing data relating to computer security incidents, as well as disseminating processed information to appropriate interested parties. The requirement for such schemes is linked to the existence of CERTs (Computer Emergency Response Teams) and other similar initiatives, the primary activity of which is to respond to security incidents with corrective action [2,3,4]. Information is obtained from member organisations (i.e. those which have an agreement with or are supported by the IRS) and presented in the form of regular reports or alerts on issues which may need immediate investigation. The reports generally reflect a large number of actual experiences from different establishments, enabling member organisations to better understand what they need to protect and why they need to protect it.

The desirability of a healthcare-specific scheme is related to both the increased use of interconnected and highly sensitive healthcare systems, as well as the characteristics of healthcare environments that set them apart in terms of other requirements for security [5].

The ISHTAR work has established a reference model in order to structure the HIRS. Its aim is to provide HCEs with facilities to compare results, improve information quality and obtain a more accurate view of the threats and vulnerabilities that member organisations are susceptible to. The main building blocks suggested in this model are incidents, threats, vulnerabilities, impacts, assets, impact metrics, user organisations, reports, and the HIRS operator. An appropriate entity relationship model has been designed to include the above concepts and their relationships. This model has been applied in the development of the HIRS database management system.

The user needs and expectations for such a HIRS were established via a short survey amongst the ten Verification Centres within the ISHTAR project (European HCEs acting as referees on the results and outcomes of the work). The centres involved employ a total of approximately 17500 employees, with individual sizes varying between 1500 and 5000 people. The requirement was determined for a pan-European HIRS, in which the security or data protection officers within the participating HCEs would submit incident notifications on a voluntary basis. Incidents would be validated with the originating HCE by the HIRS operator and the resulting reports issued immediately or periodically, depending upon the nature of the incident. Security of the process is required in terms of the communication of incidents (e.g. safeguarding the confidentiality of the HCE), as well as the storage and management of the incident database.

The resulting HIRS architecture suggests three main tasks: incident collection / notification, incident data processing by the HIRS and generation of reports. These are described in and the sections that follow.

Incident notification

The person with the responsibility for incident notification principally uses either secure e-mail or registered postage to notify the incident to the HIRS. An appropriate validation and authentication procedure is applied by the HIRS operator to verify that the notified event is a genuine incident and that it originates from the claimed HCE (avoiding the opportunity for false notifications to be submitted for malicious purposes and the like).

Incident data processing

The HIRS will process the collected incidents to produce useful and meaningful reports, enhanced with information that may stem from similar incidents that already have been registered at the HIRS database. The reference model will provide data anonymity by hiding any relative information once it is obtained by the HIRS operator. Mechanisms for achieving this focus on the encryption of names and clues concerning the HCE involved, departments and people employed. It should be noticed that the HIRS operator

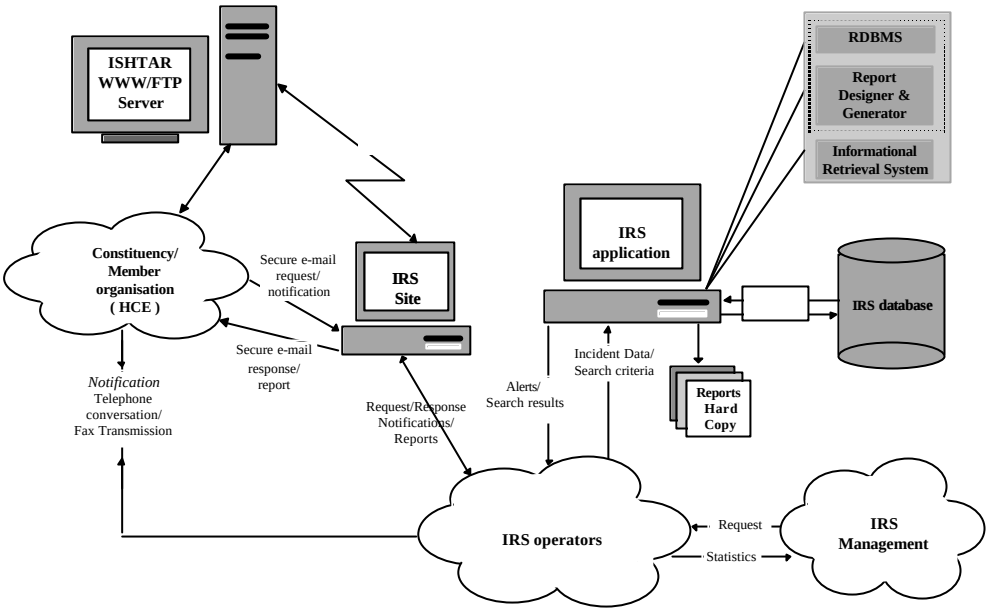

Figure 1 - ISHTAR Healthcare Incident Reporting Scheme

must comply with any terms imposed in a contractual agreement between the client-HCE and the provider-HIRS concerning the security issues. Such binding procedures will act as a deterrent to any arbitrary action taken by the HIRS operator. In addition, confidentiality will be maximised by physically isolating the HIRS database containing the actual incident data, with no network access to the machine.

Reporting

The HIRS will provide HCEs with several types of report, including alerts, statistics, regular reports, and special or ad hoc extraction reports. The HIRS operator will be able to select appropriate incidents based on a variety of criteria that more or less reflect the way data are structured inside the database. For example, the HIRS operator may select incidents based on a specific type of threat. After selecting the appropriate incidents, the operator will be able to issue a regular report or any other report based on these incidents. The reporting facility will also take account of odd incidents that may occur in different organisations but show signs of similar behaviour. A number of reports, based on anonymous incident data, will be available from the ISHTAR WWW site.

An overview of the overall HIRS process is illustrated in figure 1. Further details of the approach can be found in [6].

A pilot version of the HIRS has been developed for trial purposes within the ISHTAR Verification Centres. This is based upon a Microsoft Access 7.0 database and runs on a Pentium PC with 24Mb RAM and 500Mb of hard disk space (sufficient for 133000 incidents). The current functionality encompasses the management of the database (i.e. registration, update and deletion of incident records) and the publishing of reports (based upon a variety of criteria - e.g. incidents relating to a specific type of threat).

Healthcare Security WWW Service

Whilst the HIRS provides a means of monitoring the level of healthcare incidents and ensuring that establishments can be made aware of the possible threats, HCEs also require a means by which they can be proactive in responding to and preventing security problems. One step towards achieving such an objective is to ensure the wide availability of suitable material for guidance and awareness purposes. As a consequence, another aspect of the work being conducted by ISHTAR is the establishment of a World Wide Web service to promote healthcare security issues and accompanying advice. This is seen to represent an appropriate medium for such dissemination as it is increasingly regarded as a valid source of information and is generally accessible to the majority of healthcare establishments.

Service content and structure

The content of the WWW service can be grouped into three main categories :

1. detailed information sources;
2. reference facilities;
3. supporting services.

The detailed information sources represent the main areas from which security advice and guidance can be obtained. This category is further divided into four sections, as described below.

Healthcare Security Guidelines

A range of healthcare-specific guidelines for information systems security have been produced by the SEISMED (Secure Environment for Information Systems in MEDicine) project, a forerunner of ISHTAR under the European Advanced Informatics in Medicine (AIM) programme. These provide comprehensive coverage of a range of security issues with relevance to the healthcare community, with the following key areas being targeted [7]:

- High Level Security Policy;
- Risk Analysis;
- Security in existing systems;
- Secure systems development and implementation;
- Network security;
- Security of medical database systems;
- Use of cryptographic mechanisms.

Details of these guidelines are presented on the WWW site, providing the principal source of security advice. The majority of the information is initially presented as a series of key "advice points", but it is intended that the service will ultimately migrate to providing an integrated, full-text document set as the guidelines are updated and enhanced within the ISHTAR framework.

Verification Centre Scenarios

This section presents "roadmaps" for achieving successful security, addressing typical issues that have been faced in practice by the ISHTAR Verification Centres. The description highlight particular points that should be considered (e.g. potential problems), as well as links to the relevant guidelines.

Archive

This aspect provides a repository for papers and presentations relating to particular healthcare security issues, giving a more specific treatment of interesting areas (as generally found in journal papers or conference presentations).

Incident Reports

This section presents statistical reports and anonymised descriptions based upon genuine healthcare security incidents, drawn from the HIRS and other sources. These are intended to act the impetus for HCEs to give appropriate consideration to the "advice" aspects of the service.

The reference facilities provided by the service include an online glossary of security terminology (accessible directly or via hyperlinks from the other sections) and a bibliography of healthcare security references.

The supporting services relate to search and feedback facilities, as well as the provision of a comprehensive set of relevant links to external Internet sites.

The features described are structured into the current version of the WWW site as illustrated in figure 2. The purpose and content of the site are described in more detail in [8].

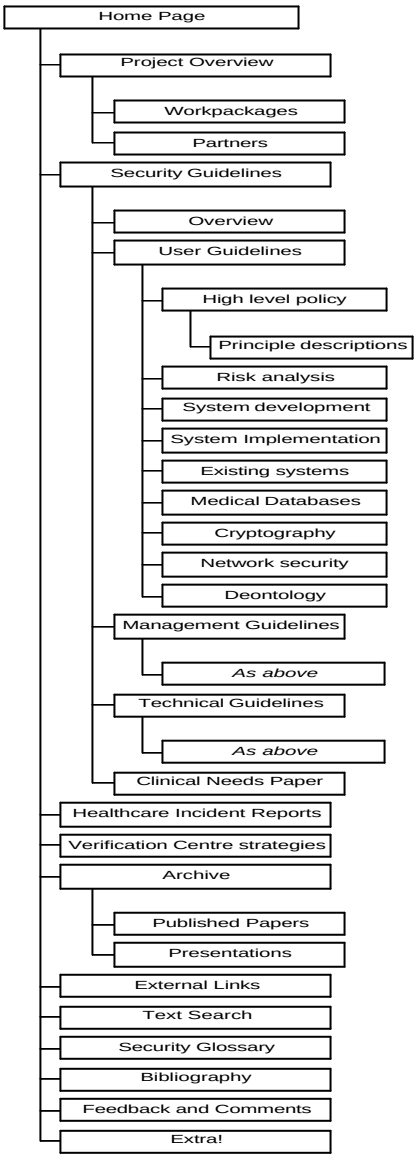

Figure 2 - ISHTAR WWW site structure

Advantages of WWW dissemination

The provision of such a site is considered to offer a number of advantages to the healthcare community. The principal point here is that the advice will be widely accessible, helping to achieve the objective of promoting security issues to a wider audience. In addition, it will represent a means of ensuring that consistent advice is provided to different establishments in relation to the same (or similar) issues. As such, the service will contribute towards the

standardisation and harmonisation of healthcare security. Finally, it is hoped that the fact that the advice is available free of charge will encourage HCEs to consult it and address their security concerns. In current scenarios, where no in-house expertise is present, HCEs must resort to utilising costly external consultancy to address the requirements. In many cases this is not practical and, as such, security issues may go unresolved or even unnoticed. This is clearly an undesirable situation and the WWW service will help to alleviate it to a certain degree.

Conclusions

Security breaches can have a number of significant consequences for a HCE, including reduced efficiency, loss of funds, damage to the organisation's reputation, reduced patient trust or even loss of life. As such, the issues of maintaining security and responding to incidents appropriately must be carefully considered.

The ISHTAR project can be seen to be making a significant contribution to these areas, providing a framework through which HCEs can both report and respond to incidents. In fact, the efforts extend beyond this in that diligent establishments may actually use the advice being offered to install countermeasures to safeguard against (or at least reduce) the likelihood of many incidents occurring.

The HIRS is being given a practical trial by the selected Verification Centres and the success of the scheme will be evaluated prior to wider deployment. The WWW site is currently operational and includes a range of useful information, as previously described. This will be updated and enhanced over time as further relevant material is produced within the ISHTAR project and within the wider healthcare security domain.

Acknowledgments

This paper has arisen from the authors' involvement in the ISHTAR Project, a Telematics Applications for Health Project (HC1028) of CEC DGXIII C.

References

[1] Audit Commission, *Opportunity Makes a Thief: An Analysis of Computer Abuse*, National Report, London, HMSO, 1994.

[2] Sparks S, Fithen K, Swanson M, Zechman P. Establishing an Incident Response Team, in *Proceedings of the 9th FIRST Computer Security Incident Handling Workshop*, Bristol, England, 23-27 June 1997.

[3] Smith D. *Forming an Incident Response Team*, ftp://ftp.auscert.org.au/security/papers/Forming_an_Incident_Response_Team_A4.ps, AUSCERT (Australian CERT), 1997.

[4] Wack JP. *Establishing a Computer Incident Response Capability (CSIRC)*, NIST Special Publication, November 1991.

[5] Roger France FH and Gaunt PN. The Need for Security - A Clinical View, in *Proc. of IMIA Conference on Caring for Health Information Safety, Security and Secrecy*, B. Barber, et al., eds., The Netherlands, November 1993.

[6] Mavroudakis KG, Katsikas SK and Gritzalis DA. Forming a Health Care Incident Reporting Scheme, in *Proceedings of Medical Informatics Europe 14th International Congress (MIE 97)*, Porto Carras, Greece, 25-29 May 1997.

[7] SEISMED Consortium. *Data Security for Health Care*. IOS Press, 1996.

[8] Furnell SM, Sanders PW and Warren MJ. Provision of healthcare security information services using the World-Wide Web, in *Proceedings of Medical Informatics Europe 13th International Congress (MIE 96)*, Copenhagen, Denmark, 19-22 August 1996.

Address for correspondence

Dr Steven Furnell, Network Research Group, University of Plymouth, Plymouth, United Kingdom.
E-mail: stevef@pbs.plym.ac.uk
ISHTAR WWW URL: http://www.ishtar.org.uk