e-Health security issues: the e-DiaMoND perspective

Mark Slaymaker, Eugenia Politou, **David Power**, and Andrew Simpson

University of Oxford

Abstract

The principle aim of the e-DiaMoND project is to develop a prototype Grid infrastructure to support the needs of the breast care community. The prototype system is but one major deliverable of the project; the other is a blueprint document that describes how a system such as e-DiaMoND might be deployed throughout the United Kingdom to support the NHS Breast Screening Programme. A key consideration of both the prototype and the blueprint document is security. We provide a summary of the generic security issues faced by e-Health projects such as e-DiaMoND.

1. Introduction

The e-DiaMoND project [1] aims to develop a prototype for a national database of mammograms that is sympathetic to the work practices employed within the UK's NHS Breast Screening Programme. The motivation for the work is derived from the fact that a large database with fast access would provide an invaluable resource to the breast imaging community by (amongst other things) aiding in the breast screening process, improving the quality of training, and providing a huge resource for epidemiological studies. The key objectives of the project can be stated thus: to build a Grid-enabled system to enable the storage and timely retrieval of mammography images and related data; to develop applications to support the processes of screening, computer aided training, computer aided detection, and epidemiology; and to develop and evaluate the effectiveness of image standardisation techniques.

In this paper document the aspects of security within e-DiaMoND that should be of interest to the wider e-Health community. This paper updates and summarises the work of [2].

2. Constraints

Within a project such as e-DiaMoND, in which there is a need to consider the requirements for potential implementation within a real clinical environment and using real patient data, the following are all key considerations.

- Ethical and legal considerations for the use of, and processing of, data for use by the project. This requires both clearance from the relevant ethics committees as well as compliance with The Data Protection Act (1998) and The Human Rights Act.
- Analysis of NHS network constraints and developing an understanding of how to work within these to ensure deployment.
- Deployment of workflow methods enabling the project to demonstrate scenarios, but offering flexibility for future exploitation.
- Understanding of the current and projected IT initiatives in the NHS and the general healthcare domain.

3. Threats

When considering the development of any security- (or safety-) critical system, one is required to undertake a thorough threat (or hazard) analysis. The National Research Council in 1997 identified five classes of threat to consider for healthcare systems. These are: insiders who make 'innocent' mistakes and cause accidental disclosures of confidential information; insiders who abuse their access privileges; insiders who knowingly access information through spite or for profit; an unauthorized physical intruder gains access to information; and vengeful employees and outsiders. All of these threats – as well as others – are of relevance to systems such as e-DiaMoND.

In addition, the project team took the following approach in determining the security requirements for the project:

- Reviewed the current initiatives within the NHS and in particular the work of the NHS Information Authority.

- Reviewed BS7799, the British Standard for the deployment of security systems and processes.
- Performed modelling of the proposed prototype and the project using methods proposed by the e-Science Security Task Force. In this respect, the team identified assets, threats to those assets, and countermeasures to secure those assets from the threats following the method proposed by Flechais and Sasse [3]. The results of this analysis are detailed in [2].

4. Functionality

Before considering security implementation issues it is worth, first, considering the functional behaviour of the e-DiaMoND system. The core e-DiaMoND system consists of middleware and a virtualised medical image store to support the concept of a data grid. The virtualised medical image store comprises physical databases, with each being owned and managed by a Breast Care Unit (BCU). The e-DiaMoND grid is formed by participating BCUs coming together as a virtual organisation, and uniting their individual databases as a single logical resource. In addition, there are a number of stand-alone databases and applications.

5. Aspects of security

Having introduced the functionality, we now consider (briefly) ten aspects of security.

Anonymisation: There is a clear need for adequate security when dealing with patient data. This need is partly driven by legal requirements as set down in the Data Protection Act, as well as ethical considerations and the need for confidentiality. It is necessary to get patient consent to use data relating to them within the e-DiaMoND project. Although the data protection commissioner is happy to accept 'implied' consent, the ethics committees tend towards needing explicit consent, with explicit opt-in rather then an option to opt-out. e-DiaMoND has to work with anonymised data: all data legally and ethically obtained, meaning all data is collected with explicit opt-in consent as required by the ethics committee. The data collected has to go through a process of anonymisation, which requires a detailed set of operating procedures to be defined along with appropriate training of those entering data.

Audit trails: There is a clear need within e-DiaMoND to record the actions of those using the system. It is intended to record both the modification of data and also the reading of data from the system. Additionally the database has been designed in such a way, that although the most up to date version of data will normally be presented, it is still possible to retrieve old versions of data.

Physical security: It is important that the equipment holding the data is protected by appropriate physical security. A minimum requirement is that the equipment is located in an area with limited access. Every entry into this area needs to be logged. A possible method of implementing this is the use of individual swipe cards and pin numbers along with CCTV or other video devices. In reality, the solution would be chosen to fit into the local NHS trusts' own security frameworks and budgets.

User authentication: There is a clear need to ensure the authenticity of requests for information. A method of user authentication is needed that imposes a minimum additional workload on the user. For doctors dynamic signature recognition may be useable as they are use to signing things. Other biometric methods may also be appropriate.

Client and server authentication: The use of proxy certificates and global to local identity mapping might be appropriate here. Part of this security policy is the use of both user and server certificates. This allows the mutual authentication of both the client and the server aspects of any transaction. It would also be beneficial if each machine on the network has its own certificate as well. This would prevent IP spoofing, where one machine pretends to have the same IP address as another trusted machine.

Security breach detection: Security breach detection is usually an after the event measure. It is however important to monitor and look for suspicious activity on the network. Alongside detecting a breach, it is also useful to have a limit on what each user can do. These restrictions can reduce the potential damage caused by intrusion.

Encrypted data movement: After the mutual authentication of both parties, they can share a suitable key for encryption of data transfer. This

works well for local transfers. If the client and server are situated at remote sites then VPN technology could be used to protect the transfer of data. The VPN creates an encrypted channel between the two participating sites, thereby preventing snooping by third parties.

Data integrity: Not only should data be encrypted, it should also be digitally signed. This signature ensures that the data received is the same as that sent. By signing the results of queries sent to the database it is also possible to be sure that any data outputted from the system can be trusted.

Availability: The availability of the data when it is required is essential for the smooth running of a BCU. The methods of ensuring this will include standard high availability techniques, including redundancy. The availability of workstations is also vital.

Access control: It cannot be predicted *a priori* what access control policies the NHS, hospital trusts, hospitals, departments, etc. may wish to impose on the e-DiaMoND data that they are responsible for. In terms of requirements, those associated with access control can be stated quite simply: the model must be flexible and fine-grained.

References

1. J.M. Brady, D.J. Gavaghan, A.C. Simpson, R.P. Highnam, and M. Mulet-Parada. e-DiaMoND: A grid-enabled federated database of annotated mammograms. In Grid Computing: Making the Global Infrastructure a Reality. Wiley, 2002: 923-943.

2. M.A. Slaymaker, E. Politou, D.J. Power, S. Lloyd, and A.C. Simpson. Security aspects of grid-based digital mammography. Methods of Information in Medicine, 2004. To appear.

3. I. Flechais, M.A. Sasse. Developing Secure and Usable Software. OT2003 (30th March - 2nd April) 2003.