e-DiaMoND: risk analysis

Mark Slaymaker. **Eugenia Politou**, David Power, Sharon Lloyd, and Andrew Simpson

University of Oxford

Abstract

The e-DiaMoND project 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. In this paper we describe the results of the threat and risk analysis process undertaken within the project. It is hoped that the findings are sufficiently generic to be of interest to the wider e-Health community.

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 we document our experiences of using the modelling method of Flechais and Sasse [3]. This paper details work previously described in [2].

2. The context

Although the e-DiaMoND project in its initial two-year phase is concerned with developing a prototype solution, the team is mindful of the need to develop in accordance with real-world requirements: scalability, forwards-compatibility and real-world constraints are all of particular relevance. In this respect, there is a requirement to establish that the system can work with not only anonymised data (which the prototype uses) but also real unanonymised data as would be used if the system were to be deployed "for real". Thus, the project has two key deliverables: a prototype system that works with anonymised data and is limited in scope, and a blueprint document that details how a system such as e-DiaMoND might be deployed within the NHS. All countermeasures identified were evaluated in relation to the constraints imposed on the project (budget, human resources, time, etc.), before determining what could be deployed in the prototype and what could be documented in the blueprint.

3. 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 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.

4. 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.

5. Security modelling

In following the modelling approach proposed by Flechais and Sasse [3], and suggested by the e-Science Security Task Force, one needs to perform several tasks. Essentially, these tasks consist of the identification of assets, the consideration of threats to those assets, and identifying countermeasures to secure those assets from the threats that exist.

Each asset was assessed with respect to the following attributes:

- confidentiality, i.e., the prevention of unauthorised disclosure of an information asset;
- availability, i.e., the prevention of unauthorised withholding of an information asset or resource both in terms of physical and software availability; and
- integrity, i.e., the prevention of an unauthorised modification of an information asset.

The importance of each attribute was then determined and ranked based on the following.

- Essential: the system should not be implemented without the relevant security in place
- High: there is a high risk to the project if we do not deploy the relevant security countermeasures
- Medium: there is an some risk to the asset if we do not deploy countermeasures.
- Low: there is very little risk to the asset so deploying security countermeasures to these assets is of a low priority.

In addition, the project team reviewed the current initiatives within the NHS (in particular the work of the NHS Information Authority) and also reviewed BS7799, which is the British Standard for the deployment of security systems and processes.

6. The process

The analysis involved gathering input from the project's key stakeholders. The process of interviewing and obtaining input from the various project collaborators proved challenging, as there were difficulties in getting some groups together because of the lack of available time. Other initial hurdles that had to be overcome included views such as "security is somebody else's problem" and "we do not have any assets". The discussions were generally lively once started, and could quickly deviate from the topics of importance. As such, we feel that a strong chairperson is essential for such meetings both to balance competing interests and to prevent degeneration into the consideration of tangential or irrelevant details.

7. Results

Employing the technique has enabled us to concentrate on securing those assets ranked essential or high. Interestingly, most assets were in fact considered essential, due to legal and ethical constraints. In this respect, the technique has been of most use to us not in *ranking* assets, but in *identifying* them.

We briefly identify below the key threats and the countermeasures that have been deployed within the e-DiaMOND project to counter them; more detailed information is available from the e-DiaMoND project web site.

Threats	Countermeasures
Human Error	Education Safety nets in software to attempt to catch human error where possible
Theft	Physical security – locked doors, cameras, physical access controls

Natural Disaster	Disaster recovery procedures.
Hacker	Network security policies and infrastructure Firewalls Stringent Access controls
DOS attack	Virus Management Patching DOS monitoring
Unauthorised Snoop	Physical security, ensure cannot pry Access controls Network security
Errors in annotations (training and screening)	Education Quality Procedures
Impersonation	secondary authentication methods Education on use of passwords and non disclosure
IP Rights infringed re software	Protect source code and executables
Software Failures	Implement version control and update management procedures
Data Corruption	Backups

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.