2012

Cloud security: A case study in telemedicine

Michael Johnstone
Edith Cowan University, m.johnstone@ecu.edu.au

Originally published in the Proceedings of the 1st Australian eHealth Informatics and Security Conference, held on the 3rd-5th December, 2012 at Novotel Langley Hotel, Perth, Western Australia

CLOUD SECURITY: A CASE STUDY IN TELEMEDICINE

Michael N. Johnstone
School of Computer and Security Science and ECU Security Research Institute
Edith Cowan University, Perth, Western Australia
m.johnstone@ecu.edu.au

Abstract

Security as part of requirements engineering is now seen as an essential part of systems development in several modern methodologies. Unfortunately, medical systems are one domain where security is seen as an impediment to patient care and not as an essential part of a system. Cloud computing may offer a seamless way to allow medical data to be transferred from patient to medical practitioners, whilst maintaining security requirements. This paper uses a case study to investigate the use of cloud computing in a mobile application for Parkinson Disease. It was found that functionality took precedence over security requirements and standards.

.

Keywords

Information systems security, cloud computing, telemedicine, applications development

INTRODUCTION

Confidentiality, integrity and availability are the core tenets of information security. Therefore, it would be expected that software systems would consider these tenets as paramount, as software is fast becoming ubiquitous. This is especially important in safety-critical domains such as military, aerospace and medical systems. Unfortunately, most software, according to Shostack and Stewart (2008), is insecure. It is noted by Johnstone (2009) that this is due to the tension between functional requirements (as seen by a customer) and security requirements (which often are not). Worse, Wysopal et al. (2007) suggest that security requirements are often omitted from requirements specifications altogether.

Medical systems appear especially problematic as their primary focus is patient care and security is either assumed or ignored (Williams, 2008). Several well-reported cases, such as Stanford Hospital's loss of 20,000 ER patient records (Moisse, 2011) and an Australian pathology laboratory's loss of patient data (Caldwell and Earley, 2009), highlight the embarrassment and loss of trust that occurs when medical data is leaked (a breach of confidentiality). Clearly the nature of the data and its intended use must determine which of the core tenets of information security would be applicable. For a real-time heart-rate monitor in an operating theatre, both integrity and availability would be critical; confidentiality less so. In an on-line web-based patient record input system, confidentiality and integrity would be dominant, with availability perhaps being not as important.

According to a recent IBIS report (IBISWorld, 2012) health and allied systems are "poised to become Australia's biggest industry division and employer well before 2050...In this division, superfast broadband will be vital in driving healthcare costs down by faster diagnostics, preventive health systems [and] *partial self-diagnostic services...*"

Software engineering as a discipline is still maturing, so it is not unreasonable that software development that focuses on security concerns is still in its infancy. There is certainly evidence of an evolution from object-orientation in the 1980s, component-based software engineering in the 1990s, service-oriented architectures in the 2000s to cloud computing now. Given that cloud computing in its most basic form provides a façade for data storage and retrieval, it can provide seamless access to data which could make data management simpler and thus potentially improve information technology security management, especially as both patients and medical practitioners make increased use of wireless transmission of data and Internet-based applications.

This paper describes the issues involved with medical systems and the concomitant standards that apply to the development and use of such systems, explains the theory behind cloud computing and how this may benefit medical systems, uses a case study to illustrate the effectiveness of cloud-based data storage and retrieval for medical data and concludes by considering some security weaknesses of cloud computing.

SECURITY STANDARDS AND MEDICAL SYSTEMS

Mizukura *et al.* (2009) proposed a home health care network based on the IEEE 11073 standard. ISO/IEEE 11073 is actually a family of health informatics standards, for example, 11073-10407 specifies the behaviour of

blood pressure monitors. Mizukura *et al.* field-tested a health monitoring application that was designed to capture heath data from elderly patients in their own environment and transmit such data across a network to relevant medical practitioners.

Significant progress has been made on issues related to how to transfer medical data. For example, ISO/IEEE 11073-20601 (2010, p1) defines an abstract model of personal health data as well as the appropriate transport independent transfer grammar required to set up logical connections between systems. Such standards are being implemented by manufacturers of telemedical equipment (see, for example, Biotronik, 2011).

ISO 27799 (2008) recognises the problem and states "The need for effective IT security management in healthcare is made all the more urgent by the increasing use of wireless and Internet technologies in healthcare delivery. If not implemented properly, these complex technologies will increase the risks to the confidentiality, integrity and availability of health information."

ISO 27799 provides guidance about what sort of health data needs to be protected, but like many standards, is descriptive, rather than prescriptive. For example, it declares that personal health information (such as that collected by the iPad app described later in the case study) needs to be protected, but does not specify the precise means of protection that would meet the standard.

HL7 V2 is an OSI level 7 (hence the name) ANSI standard protocol for communication between health service providers in Australia. It offers security checks, participant identification, availability checks, negotiating exchange mechanism negotiation and provides a standard data structure. Whilst HL7 messages are text-based (and thus perhaps lend themselves to encoding in XML and transmission via SOAP), the HL7 protocol does support the transfer of picture data via Base64 encoding of the binary data stream. Whilst there is a clearly defined structure or ontology for HL7 messages, there is no innate formatting or defined dependency between the data in the observation (OBX) segments of a results message.

HL7 supports the encoding of patient identifiers, provider identifiers and observations (medical test results), whilst at the lowest level, recognises message start and end identifiers as well as individual unique message identifiers (to ensure that collisions do not occur) and acknowledgments (although it is more correct to say that an HL7-compliant application recognises the message identifiers and processes them accordingly).

Having examined some of the relevant standards and protocols for the transmission and storage of medical data, it is now appropriate to discuss how those data could be stored using cloud-based services.

CLOUD COMPUTING

As mentioned previously, cloud computing represents an evolution in the provision of software services, rather than a revolution. However, as with any "new" concept, there is sometimes confusion as to what it actually represents and what benefits might accrue from the use of such technology. In this section cloud computing is defined, the architecture of a cloud-based system explained and various models of cloud computing are discussed.

Conventionally, cloud computing appears to be focussed on large-scale storage of information across multiple servers. NIST (Mell and Grance, 2011, p2) provide a succinct definition of cloud computing that encompasses more than just distributed storage, viz: "…a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction".

Badger et al. (2012) claim that cloud computing has essential characteristics that differentiate it from earlier models of distributed computing, viz: on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service.

NIST (Badger et al., 2012) also suggest a range of service and deployment models that provide coverage of the cloud computing landscape. The service models include not only the familiar software as a service (SaaS), but also platform as a service (PaaS) and Infrastructure as a service (IaaS). PaaS encompasses software platforms (such as .NET), database engines and operating systems. IaaS provides CPUs, virtualisation (if required) and block storage. An example architecture is shown in figure 1. Clearly, one of the main advantages of a multi-layered architecture is the ability to fine-tune resource pooling in the middle layers to effect a change in performance without the service user being aware of the change (apart from the observed performance boost). Whilst resource pooling is usually a benefit as it provides redundancy, it will be shown in a later section that there are security implications with the complex architectures that are used to deliver cloud services.

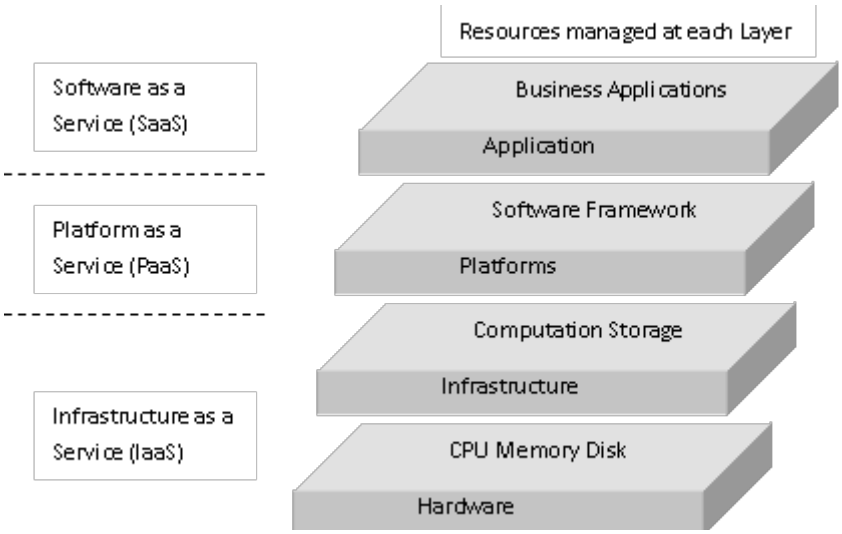

Figure 1: Clould Computing Architecture (adapted from Zhang et al., 2010).

The deployment models proposed by Badger et al. (2012, p2-2) are private, community, public and hybrid clouds. Clearly, a private cloud exists for the use of one consumer (business) exclusively. The cloud may be used by many business units within the same enterprise but the service provision may, in fact, be outsourced to a third party (which is likely and therefore the infrastructure is also likely to be remote from the consumer). A community cloud is similar except that the consumer in this case is a group of interested parties that are not from the same enterprise. The service may be managed by one of the parties in the community or by a third party. A hybrid cloud, as the name implies, can use a combination of any of the three aforementioned deployment models. The models remain distinctive but are linked by standards or proprietary systems that permit data and/or application portability.

Having defined cloud computing and discussed various service and deployment models in general, what follows is a case study which uses cloud-based services to share medical data between interested parties.

A PARKINSON DISEASE iPAD APP: A CASE STUDY

The scope for this system was to provide a proof-of-concept iPad application (app) that allowed patients with Parkinson Disease to perform several tests which provide diagnostic information and allow the test results to be shared with a neurologist, hence facilitating management of the disease. The major benefit is that patient does not need to travel to see their neurologist to perform the tests. Given that a large proportion of patients are in the 70-79 age group (Brown, 2002), the ability for the system to link to a neurologist and transfer data seamlessly was a prime requirement. By conforming to Apple's Human Interface Guidelines, it was expected that this requirement could be met, provided that the cloud services could be implemented for an iPad. Figure 2 and figure 3 show some sample screen shots of the app.

The basic requirements were to provide an app that allows a patient to perform two diagnostic tests, allow one or more of those tests to be saved and stored locally, to provide summary statistics and relevant graphical feedback to a patient so that s/he may track his/her progress and (critically for this discussion on information security) allow the sharing of patient data between one or more parties (usually the patient's neurologist) in a seamless and transparent way.

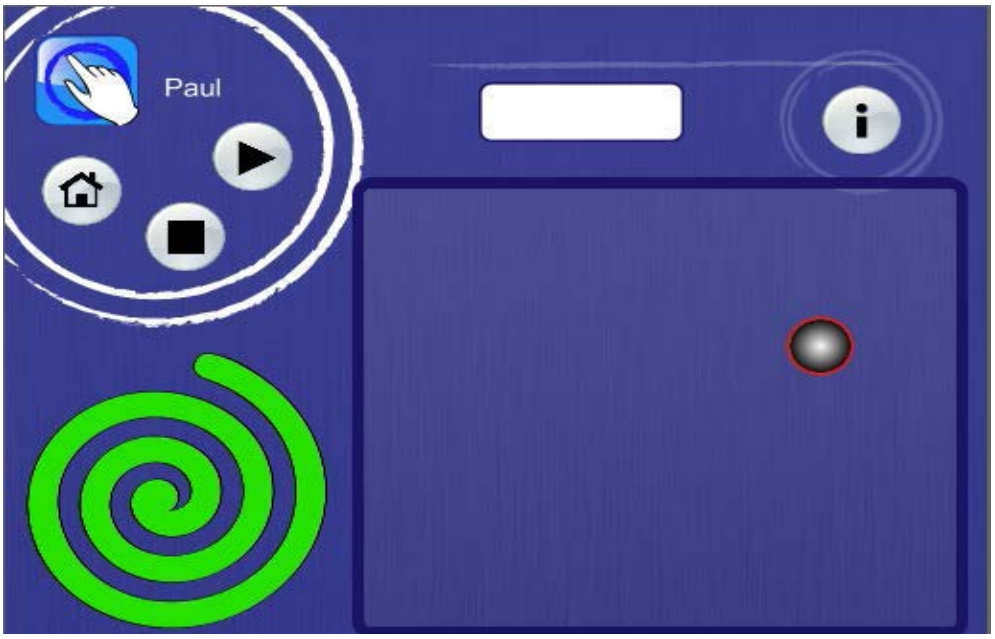

Figure 2: Sample Test from the Parkinson Disease Tester App.

Cloud computing was deemed to be a potential solution to the last requirement. The sharing requirement had to allow a patient to send a share message to another iPad user, for the second user to respond in the affirmative (or negative) to allow the transfer of patient data and for the first user to have the ability to rescind the original sharing request and thus break the connection. Several cloud providers were investigated including iCloud, Google, Nuvolabase and Moai. iCloud was an obvious first choice as the target device was an iPad, but this service is meant to be a personal cloud service used across many devices. It is not designed for sharing files with multiple users. The other cloud services were evaluated, the result being that the Moai cloud, despite being targeted at the gaming community, met all of the functional requirements and thus was selected as the cloud service for this application.

The app works by storing local data using SQLite (chosen because it doesn't require a database server), the data is stored in the cloud as a JSON (JavaScript Object Notation) file and accessed using RESTful services (common to most Web applications). JSON is a text-based standard (see RFC 4627) for defining and sending structured data between a Web application and a server. JSON provides the usual data types (number, string, Boolean, array and object). A JSON structure for the iPad app test data object is:

```
"test": [
        {
      "type": "spiral",
      "number": "20",
      “date”: “20121009”,
      “value-array”, [4,6,5,3,3,7]
        },
        {
      "type": "countdown",
      "number": "6"
      “date”: “20121009”,
      “value”: “13”
        }
    ]
```

In this structure there are two types of test and whilst they share some common data elements such as a test number and a test date, the actual results are different. JSON is able to characterise these different structures easily and thus is a good choice for representing the ontology of a test.

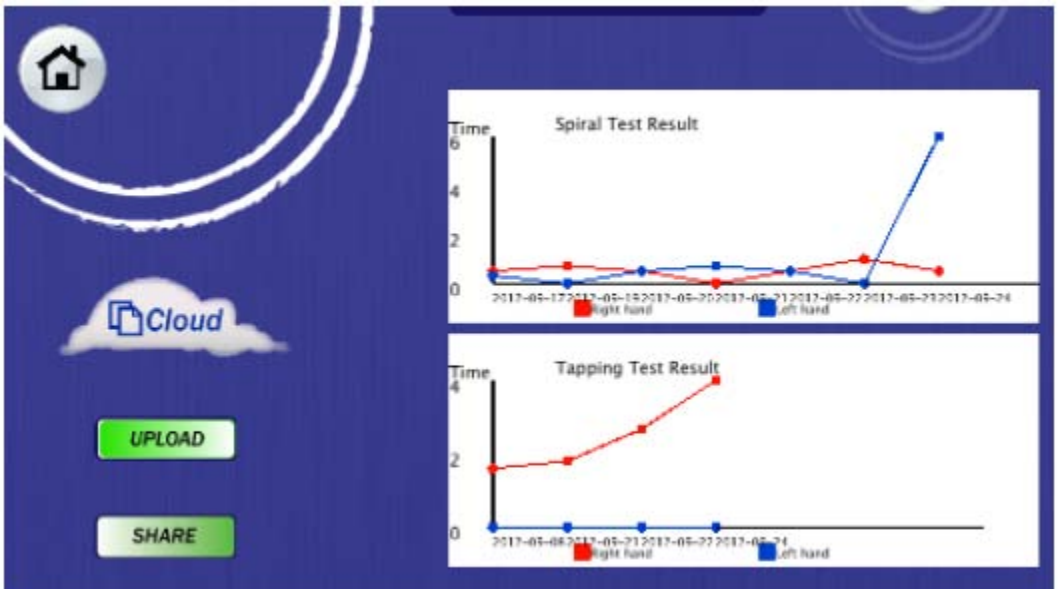

Figure 3: Sample Output from the Parkinson Disease Tester App.

ANALYSIS AND DISCUSSION

Considering cloud computing in its simplest (conventional) incarnation, which of distributed file storage and retrieval, there are several aspects of confidentiality, integrity and availability that are worth discussing. If patient data is stored unencrypted on a cloud-based file system this would appear, at first glance, to be a breach of confidentiality as the file is stored in plain text (plain text in this context does not necessarily refer to ASCII text, but to any non-encrypted form of data, for example human-readable XML records, Microsoft Word documents or the data referred to in the case study). Confidentiality is maintained by two means. First, the user does not know which physical location stores the data and second, the data may be split into several parts across several locations. The semblance of a single file is maintained by the cloud façade as part of SaaS (as shown in figure 1). Integrity appears problematic by virtue of the benefits which assure confidentiality, that is, the separation of the file into multiple parts across multiple locations. Provided that the PaaS layer is intact, the marshalling of the file from its parts into a whole is transparent to an end-user of the cloud. Availability is, of course, handled by the IaaS layer.

This describes the scenario where all of the components of cloud computing work seamlessly to provide the services expected of them. From a security perspective, it is worth examining how standard attacks on confidentiality, integrity and availability might affect the provision of cloud services. A standard attack on availability is denial-of-service (DoS). Figure 4 indicates an alarming trend. DoS attacks are increasing, not in complexity, but in their size. This means that a DoS attack on a cloud service provider will almost certainly result in a loss of availability. The wider problem is that the outcome of a DoS attack may affect integrity if a file is partially constructed. There may be the opportunity for the data to be modified or for data to be leaked (a breach of confidentiality) because of a failure in the other service provision layers.

Turning now to the specifics of the case study, a well-trodden mitigation pathway for problems of confidentiality is encryption. Certainly the data being transferred from an iPad to the Moai cloud could be encrypted before transmission from a patient's iPad and storage and decrypted on retrieval on a neurologist's iPad. Whether a public key infrastructure or private keys are chosen is perhaps not an issue as long as the key length prohibits the data being compromised during its effective lifetime, notwithstanding the key transmission safety issues inherent in the sharing of private keys. Integrity issues are often dealt with by the use of cyclic redundancy checks or hashing. Both techniques are feasible with the data being transferred from the iPad to the cloud. It requires that the PaaS layer be capable of forming and sending a re-transmission request if data were found to be corrupt. Availability issues appear the most insoluble in this scenario because of the ease by which DoS attacks can be mounted. It is possible that IPv6, with its significantly larger address space (as compared to IPv4) may provide a successful mitigation strategy.

Rather than using JSON as the messaging format, HL7 could provide a better alternative. One possible mapping of an observation or OBX record (diagnostic test result) equivalent to the aforementioned JSON representation is:

```
OBX-2 (Value type) NM                                  // a number
OBX-3 (Observation ID) 6^Countdown^LN                  // the type of test
OBX-5 (numeric) 13                                     // the actual value
OBX-6 (units) s^Seconds^ISO+                           // units of the value
OBX-14 (date/time of observation) 20121009+1000
```

On its own, the use of HL7 over JSON does not appear to provide significant benefits. In terms of message transfer between a patient and a neurologist the overheads for HL7 are greater but there are some security advantages as mentioned in a previous section. Remembering that the app is designed to share data in a one-to-many relationship, the real benefit to using HL7 is realised when several health care providers wish to share data about the same patient. In this scenario, using a common protocol designed for health data makes the translation and interpretation of the data relatively straightforward.

The benefit of the cloud in terms of hiding the physical location/structure of the file becomes problematic when confidentiality is breached at the lower levels of the cloud architecture (figure 1). This is largely because, especially in a hybrid deployment, multiple stakeholders across multiple domains may share physical data space. In contrast to a more conventional model of data storage where a stakeholder has access to contiguous space, in the shared (cloud) space, parts of files may be juxtaposed with data from other stakeholders. This leads to questions about effective access controls and authentication mechanisms at the higher levels of the cloud architecture. The implementation of such controls and mechanisms is non-trivial.

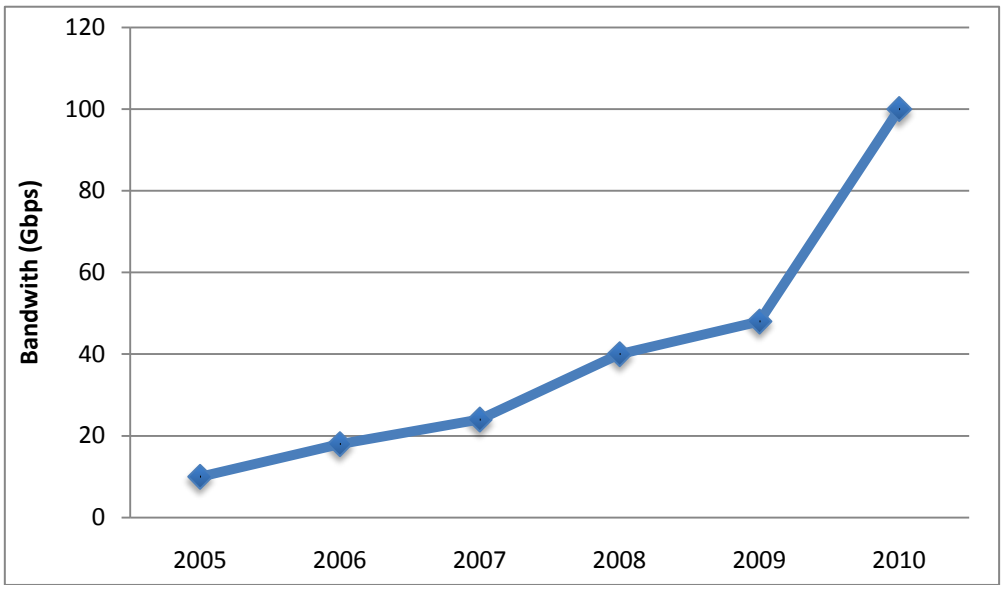

Figure 4: Largest Single Denial of Service Attack (Arbor Networks, 2010, p5).

In summary, the difficulties in guaranteeing cloud service security were discussed and a case study which highlighted some of the likely problems to be encountered in the hosting of medical data was put forward. Ultimately, it may be that experience in secure development as applied to the domain of cloud computing is the key determinant of the success of any remote hosting and transfer of any medical information.

CONCLUSIONS AND FURTHER WORK

This study explored the problems of using a nascent technology, cloud computing, to store medical data. The complex nature of cloud services was revealed and a case study that described the implementation of an iPad app that transferred medical data was articulated and discussed.

Specifically, this study used a case study to show how a medical data could be generated, stored and shared using cloud computing. It was argued that cloud services provided benefits in that the cloud façade hid the complexity of data transfer and storage from the end-user, as compared to conventional database or file-based storage techniques. It was shown that the cloud could inadvertently be responsible for security breaches under certain circumstances.

A limitation of this work is that it used only a single case study with a specific cloud platform, therefore it would be unwise to conclude that all cloud platforms or deployment models suffer from identical security

problems. Further work would involve extending this idea to see how well other cloud providers dealt with the security issues outlined in this paper.

REFERENCES

Badger, L., Grance, T., Patt-Corner, R. and Voas, J. (2012). "Cloud Computing Synopsis and Recommendations.". NIST Special Publication 800-146.

Biotronik. (2011). BIOTRONIK Home Monitoring EHR DataSync Documentation of the BIOTRONIK IEEE 11073-10103 XML Structure: Technical information for software developers and system architects. Berlin, Germany: BIOTRONIK SE & Co. KG.

Brown, I. (2002). "Does caffeine protect against Parkinson's disease? A preliminary study", *Nutrition & Food Science*, 32(6), 227-30.

Caldwell, A. and Earley, D. (2009). Patients' medical records leaked online by pathology lab Sullivan Nicolaides. Retrieved from http://www.news.com.au/technology/patients-medical-records-leaked/story-e6frfro0-1225699562788

IBISWorld (2012). *A Snapshot of Australia's Digital Future to 2050*. IBIS Publishing.

ISO/IEEE 11073-20601 (2010). *Health informatics — Personal health device communication — Part 20601: Application profile — Optimized exchange protocol*. New York, NY: Institute of Electrical and Electronics Engineers, Inc.

ISO 27799 (2008). *Health informatics — Information security management in health using ISO/IEC 27002*. Geneva, Switzerland: International Organisation for Standardisation.

Johnstone M.N. (2009). "Security Requirements Engineering-The Reluctant Oxymoron." *Proceedings of the 7th Australian Information Security Management Conference*, Edith Cowan University, Perth Western Australia, 1st-3rd December 2009.

Mell, P. and Grance, T. (2011). "The NIST Definition of Cloud Computing.". NIST Special Publication 800-145.

Mizukura, I., Tamura, T., Kimura, Y. and Yu, W. (2009). New Application of IEEE 11073 to Home Health Care. *The Open Medical Informatics Journal.* 3: 44-53.

Moisse, K.. (2011). Stanford Hospital Patient Records Leaked Online. Retrieved from http://abcnews.go.com/blogs/health/2011/09/09/stanford-hospital-patient-records-leaked-online/

Shostack, A. and Stewart, A. (2008). *The New School of Information Security*. Upper Saddle River, NJ: Addison Wesley.

Williams, T. (2008). When trust defies common security sense. *Health Informatics Journal*, 14(3), 211-221, Sage Publications London.

Wysopal, C., Nelson, L., Dai Zovi, D. and Dustin, E. (2007). *The Art of Software Security Testing*. Upper Saddle River, NJ: Addison Wesley.

Zhang, Q., Cheng, L. and Boutaba, R. (2010). "Cloud computing: state-of-the-art and research challenges." *Journal of Internet Services and Applications.* 1(1): 7-18.