Security Considerations for Tablet-based eHealth Applications

Martin Gilje Jaatun[1], Ellen A.A. Jaatun[2], and Russ Moser[3]

[1] Department of Software Engineering, Safety and Security
SINTEF ICT
NO-7465 Trondheim, Norway
martin.g.jaatun@sintef.no
http://www.sintef.no/ses
[2] Faculty of Medicine, Department of Neuroscience
NTNU
Trondheim, Norway
ellen.jaatun@ntnu.no
http://www.ntnu.no/
[3] Telltale Solutions
Maine, USA
russellmoser@gmail.com

Abstract. Tablet computers are slowly being put into use in hospitals and primary care both by clinicians and patients. This paper will examine security needs of tablet-based eHealth applications, and explore how conventional security mechanisms can be adapted to this space. Our approach will be demonstrated by examining a particular eHealth application; a tablet-based Pain Body Map for use in palliative care.

Keywords: Security, eHealth, tablet, Pain Body Map, PBM

1 Introduction

Tablet computers such as the Apple iPad are increasingly being used in healthcare settings; recent figures estimate that there are in excess of 12000 healthcare-related apps in Apple's iTunes store, and three or four times as many when counting also other mobile platforms [1]. Surveys show, however, that the ease of use of tablets is offset by security concerns regarding potential loss of confidential medical information on mobile devices [1].

In: E.A.A. Jaatun, E. Brooks, K. Berntsen, H. Gilstad, M. G. Jaatun (eds.): Proceedings of the 2nd European Workshop on Practical Aspects of Health Informatics (PAHI 2014), Trondheim, Norway, 19-MAY-2014, published at http://ceur-ws.org

In this paper we will discuss a set of reusable security requirements proposed for eHealth application, and examine how these requirements can be met by tablet computers in general, and in particular by one specific eHealth application; a tablet-based Pain Body Map (PBM) for use in palliative care.

The remainder of this paper is structured as follows: Section 2 gives an overview of information security threats towards eHealth applications. Section 3 presents an example tablet-based eHealth application that we will use to examine security needs and subsequently a security solution. Section 4 summarises the security offered by one specific tablet platform, i.e., the Apple iPad, and provides recommendations for how it best can be configured to offer optimal security. Section 6 discusses how our example application addresses the security needs of en eHealth platform, and Section 7 concludes the paper.

2 Background

It has been claimed that the form factor of mobile devices in itself represents an improved physician-patient relationship [2]. Many eHealth applications used in a clinical setting are therefore being developed on a tablet-based platform.

Jones et al. [3] discuss privacy and security of an iPad-based health application, but focus almost exclusively on the problem of sensitive information being entered on the iPad in a public setting, and thus risking that bystanders might be able to read sensitive information as it is being entered. In our paper, the focus is rather on the security of information *after* it has been entered.

Health information is a perfect example of the kind of sensitive personal information that is protected by the European Privacy Directive [4] and similar legislation. The introduction of the Health Insurance Portability and Accountability Act (HIPAA) in the US also introduced more focus on the need for information security in health settings [5]. Healthcare applications are thus subject to a number of security requirements, and based on the European Privacy Directive, Jensen et al. [6] enumerated a set of reusable security requirements for eHealth applications which we reproduce here:

1. Services should identify and verify the identity of all of its human users before allowing them access to their resources.
2. Services should identify and verify the identity of corresponding services before they are allowed to communicate.
3. Services should verify the authorisation level of users before access to sensitive data can be given.
4. The platform should support integrity protection of sensitive personal data while it is stored.
5. The platform should be able to detect unauthorised manipulation of data that is being transmitted.
6. The platform must protect any stored sensitive personal data from unauthorised access.
7. Personal sensitive data must be confidentiality protected while transmitted over open, untrusted communication lines.

8. The platform should be able to log security incidents, such as failed login attempts or unauthorised access attempts to services in order to discover and trace system abuse.
9. The platform should be able to log activities related to access of sensitive information.
10. Input validation should be performed at time of data reception to reduce threats represented by malicious content and malformed packets.
11. Multiple levels of security should be ensured to avoid a single point of failure.
12. Data freshness should be controlled to prevent chances of replay attacks.
13. A patient journal should show who has added content, e.g. through electronic signatures.

In the following we will discuss how these requirements relate to tablet-based eHealth applications, and to what extent the available security mechanisms can fulfil them.

3 Example Application - Pain Body Map

In this section we will describe an example application that has been developed for a tablet computer to be used in a clinical setting. Fig. 1 shows an iPad-based Pain Body Map (PBM) for use in palliative care [7, 8].

3.1 Why Pain?

Pain is a common problem for patients with advanced cancer in palliative care. These patients are taken care of by many healthcare professionals, in many different settings. Most of the time, these patients are in their own homes, and in many cases pain management can be very challenging. Pain is a very abstract phenomenon which can be clear interpreted when you are experiencing it. Describing it to a third person is challenging due to the lack of a common description. The process of pain management require pain assessment. close collaboration between patients and health care workers. The Assessment is defined as “an ongoing and dynamic process that includes evaluation of presenting problems, elucidation of pain syndromes and pathophysiology, and formulation of a comprehensive plan for continuing care” [9]. This process requires continuous sharing of data and building a data bank based on previous pain measurements. It also requires elucidation of pain measures in order to find the cause for the pain and trace changes and their cause. This process is difficult to document and facilitate with a paper format, and a digital pain assessment tool was thus developed for standardising the process of assessment, facilitating sharing of data, and making longitudinal data better accessible.

3.2 Development of the PBM

The patients with palliative needs are taken care of by pain specialists, other specialists or a general practitioner in an in- or out-patient setting. Today PBMs

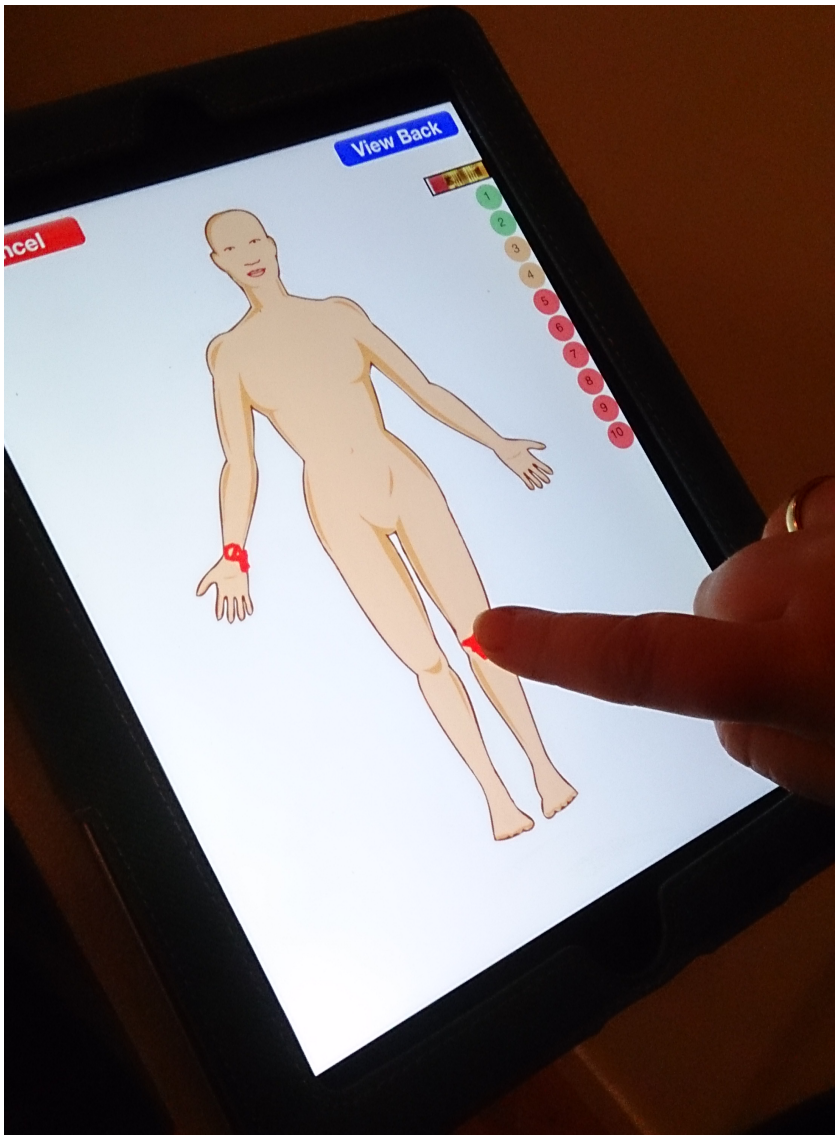

Fig. 1. An iPad-based Pain Body Map

are either used alone or as an integrated part of several different assessment tools [10, 11].The McGill pain questionnaire can be used for follow up on pain management or to identify different pain descriptions who can be representative of different pain types or pain syndromes. The Brief Pain Inventory (BPI) can also be used to follow up on pain management as it assess pain interference and pain severity. Pain intensity and pain location are considered two of the most important pain domains which can shed light over the pain severity and show changes over time [12, 13].

In clinical practice, pain is normally assessed by a nurse using a questionnaire before the patient gets to talk to the physician. The data is presented to the physician, and used for better understanding the patient's pain problem. The questionnaires should be saved and used to see changes over time. In this way the health care professional can see the results of the pain management. The assessment can be used in both in- and out-patient settings.

We based our development on an agile user centred development process. Requirements for the PBM was based on a usability testing of a Computerised Pain Body Map made for a laptop computer [14]. Based on the requirements we decided to use the iPad as platform and develop the program as an iPad application.

3.3 Using the PBM

The PBM can be used in a hospital setting, but also in ambulatory out-patient care, and could even be used by patients for extended-period self-reporting. We are currently limiting the discussion to tablets managed by an enterprise solution, which implies that any use of personally owned tablets are out of scope for this paper.

4 Security Mechanisms Offered by the iPad

The key to secure use of iPad and other tablet devices is to make it part of an enterprise solution [15, 16], where organisational security policies can be enforced. There are a number of security mechanisms that can be deployed on the iPad platform, but in the following we will concentrate on those that are most relevant to a mono-purpose healthcare application.

4.1 Password Protection

Any iPad used in a clinical setting should be forced to set an enterprise password and automatic screen locking. Although it is currently most common only to use a simple PIN for this purpose, the iPad supports using a proper full-length password [15], something which highly desirable for devices which may contain information from multiple patients[4].

[4] Tablets used by individual patients in their own home have their own challenges, but this is out of scope of this paper.

4.2 Encryption

The iPad can be configured to encrypt all persistent data using a key based on the unlock PIN or password. This should be the default configuration for any tablet used in an eHealth setting, enforced via the aforementioned enterprise solution.

4.3 General Hardening

A typical problem with portable general-purpose computing devices is that the temptation to use them for personal purposes is significant. For tablet devices, there further seems to be a lower psychological barrier to installing new software than on a desktop computer; some users even seem to think that there is a difference between an "app" and a "program". This may be a problem, since both iTunes and the Android appstore have contained apps that contained malware or spyware [17, 18]. The US National Institute of Standards and Technology (NIST) has published a very useful guide for secure use of mobile devices [16], and many of their recommendations also apply to the iPad and other tablets.

If a tablet is to be used in a clinical setting, we recommend removing all non-essential apps, as well as disabling the appstore (preventing the user from installing new apps). Alternatively, the iPad could be restricted to only using a specific enterprise appstore with approved apps. Also, all general-purpose web browsers should be removed if not explicitly needed by the clinical application, or at the very least restricted to accessing specific sites in accordance with the intended use of the tablet.

The enterprise solution should also enable remote wiping in case the tablet is lost or stolen. Wiping could also be initiated in case of repeated unsuccessful authentication attempts, although it might be sufficient to lock the device in such cases; only unlocking from the enterprise solution when it is verified that the tablet is in the possession of an authorised user.

The tablet should be configured to not synchronise with unauthorised computers, and only allowed to connect to specific, white-listed network services using an encrypted connection (e.g. using a Virtual Private Network solution).

5 Additional Security Mechanisms for Tablet Devices

Each individual application (or "app") can encrypt all the data it stores based on, e.g., an application-specific password. This would make it possible to provide additional protection at an arbitrary level, without being restricted by what the underlying operating system offers. In this solution, it would be required to provide a password to access the stored data.

If a network connection is available, the eHealth application could be configured to not store data locally, but upload everything to a secure server. The conventional way of securing such communication is by using SSL/TLS, where appropriate configuration of allowed cipher suites can ensure adequate protection. However, if a tablet is to be used in an outpatient setting, a network

connection can not always be relied on; even in a prosperous country such as Norway there are still dead spots without even cellular coverage. This implies that the tablet will need to store certain amounts of patient data locally, at least until it returns to the enterprise environment (e.g., the hospital), which means that appropriate measures as indicated above need to be applied.

Many tablets can be fitted with a GSM/UMTS Subscriber Identity Module (SIM), allowing them to communicate using GPRS or UMTS data communication. Although such communication typically is encrypted, it is important to know that the level of security offered actually can vary from operator to operator [19]. For healthcare applications, it is therefore not advisable to rely solely on the network-level encryption offered, but ensure that additional application-level encryption is employed when transmitting data from the tablet.

Finally, there are a number of commercial add-on packages that can provide further security features to tablets; little objective information is currently available for these solutions, so a comparison of pros and cons remains as further work.

6 Discussion

Since tablets have such a convenient ultra-portable form factor, there is increased risk that a tablet might be left behind in aircraft seat pockets, taxis and restaurants [16]; thus, protecting the data at rest on the tablet is of prime importance. However, it is also important to protect against eavesdropping on data transfers, and prevent remote compromise via malware or other means.

Considering the requirements outlined by Jensen et al. [6], we can argue that most (but not all) can be met by the mechanisms described above (see Table 1 for a summary of the following discussion).

Requirements 1 and 3 can be said to be fulfilled implicitly, since a proper password will prevent anyone than the authorised user to access the table. Organisational policies must then deny sharing of tablets. Requirements 4 and 6 are fulfilled by the password protection, encryption of stored data, and restriction of which devices the tablet may be synced with. Requirements 2, 5 and 7 is covered by restricting the tablet to communicating only with the enterprise network, protecting the connection with SSL/TLS, and requiring mutual authentication before data is transmitted. Requirement 11 is addressed by employing both device or operating system encryption, and application-specific encryption, although there may be other single points of failure that are not covered. Requirement 12 is handled sufficiently by using SSL/TLS on all network connections.

The audit requirements 8 and 9 are currently not handled in a satisfactory manner by tablet devices, although a tablet may be configured to lock after a specified number of failed logins. However, it can be argued that since a tablet in general will not be remotely accessible and only used by a single individual, the audit requirements might be less critical. The input validation requirement 10 is also not addressed, but may be less relevant since we recommend restricting which hosts the tablet should be allowed to communicate with. Finally, require-

ment 13 is currently not addressed, although it might be possible to tag (and sign) data collected on the tablet to allow tracing it back to the tablet user. However, this would require modifications to the eHealth application used on the tablet.

It should be noted that Jensen et al. [6] did not intend for their list to be exhaustive, but we nevertheless find it encouraging that the majority of their example requirements can be fulfilled in a satisfactory manner by a tablet device. We should also not forget that security is a *process*, and no solution will ever be secured once and for all. No security mechanisms can be assumed to offer perfect security, and certainly not for all time. This should be evident from the recent revelation of the Heartbleed bug, which had left OpenSSL implementations vulnerable for two years [20].

Table 1. Summary of how the example application addresses security requirements [6]

Req#	**Requirement**	**Tablet approach**
1	Verify identity of users	Password and organisational policies
2	Verify identity of services	Restrict to enterprise network, SSL/TLS, mutual authentication
3	Verify authorisation level of users	Password and organisational policies
4	Integrity protection at rest	Password protection, encryption, sync restriction
5	Integrity protection in transit	Restrict to enterprise network, SSL/TLS, mutual authentication
6	Access control	Password protection, encryption, sync restriction
7	Confidentiality in transit	Restrict to enterprise network, SSL/TLS, mutual authentication
8	Log security incidents	(Not addressed - less relevant)
9	Log access to information	(Not addressed - less relevant)
10	Input validation	(Not addressed - less relevant)
11	Multiple levels of security	Both OS and application-specific encryption
12	Data freshness	SSL/TLS
13	Non-repudiation	Not addressed

Our example application uses the iPad platform, and it is clear that the closed software model employed by Apple does make it easier to lock down the security of an iPad in an enterprise setting than, e.g., for the open Android platform. However, for the latest Android versions, the enterprise device management options[5] seem to be on par with that available for iOS, and once installing new apps is denied by policy, the point about more malware on Android [17] than on iOS is moot.

[5] http://developer.android.com/training/enterprise/device-management-policy.html

7 Conclusion

With correct configuration, tablet devices such as the iPad can now offer sufficient security to be used in eHealth scenarios. However, there is still room for improvement, in particular on the logging side, where there is currently little built-in support. Current tablets should only be used by a single healthcare worker, and should be wiped of all stored data before being reassigned.

References

1. West, D.M.: How Mobile Devices are Transforming Healthcare. Issues in TECHNOLOGY Innovation (18) (2012)
2. Alsos, O.A., Das, A., Svanæs, D.: Mobile health it: The effect of user interface and form factor on doctorpatient communication. International Journal of Medical Informatics **81**(1) (2012) 12 – 28
3. Jones, J.F., Hook, S.A., Park, S.C., Scott, L.M.: Privacy, Security and Interoperability of Mobile Health Applications. In Stephanidis, C., ed.: Universal Access in Human-Computer Interaction. Context Diversity. Volume 6767 of Lecture Notes in Computer Science. Springer Berlin Heidelberg (2011) 46–55
4. : Directive 95/46/ec (1995)
5. Baumer, D., Earp, J.B., Payton, F.C.: Privacy of Medical Records: IT Implications of HIPAA. SIGCAS Comput. Soc. **30**(4) (December 2000) 40–47
6. Jensen, J., Tøndel, I.A., Jaatun, M.G., Meland, P.H., Andresen, H.: Reusable security requirements for healthcare applications. In: Availability, Reliability and Security, 2009. ARES '09. International Conference on. (March 2009) 380–385
7. Jaatun, E.A., Haugen, D.F., Dahl, Y., Kofod-Petersen, A.: Proceed with caution: Transition from paper to computerized pain body maps. Procedia Computer Science **21**(0) (2013) 398 – 406 The 4th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN-2013) and the 3rd International Conference on Current and Future Trends of Information and Communication Technologies in Healthcare (ICTH).
8. Jaatun, E.A.A., Haugen, D.F., Dahl, Y., Kofod-Petersen, A.: An improved digital pain body map. In: e-Health Networking, Applications Services (Healthcom), 2013 IEEE 15th International Conference on. (2013) 697–701
9. Hanks, G., Cherny, N.I., Christakis, N.A., Fallon, M., Kaasa, S., Portenoy, R.K., eds.: Oxford Textbook of Palliative Medicine. 4 ed. edn. Oxford University Press (2009)
10. Melzack, R.: The McGill Pain Questionnaire: major properties and scoring methods. Pain **1**(3) (September 1975) 277–299
11. Cleeland, C.S., Ryan, K.M.: Pain assessment: global use of the Brief Pain Inventory. Ann Acad Med Singapore **23**(2) (1994) 129–38
12. Hølen, J.C., Hjermstad, M.J., Loge, J.H., Fayers, P.M., Caraceni, A., Conno, F.D., Forbes, K., Furst, C.J., Radbruch, L., Kaasa, S.: Pain assessment tools: is the content appropriate for use in palliative care? Journal of Pain and Symptom Management **32** (December 2006) 567–580
13. Jaatun, E.A.A., Hjermstad, M.J., Gundersen, O.E., Oldervoll, L., Kaasa, S., Haugen, D.F.: Development and testing of a computerized pain body map in patients with advanced cancer. Journal of Pain and Symptom Management **47**(1) (2014) 45–56

14. Jaatun, E.A.A., Haugen, D.F., Hjermstad, M.J., Kaasa, S., Gundersen, O.E.: Acceptability and Validity of a Computerised Body Map for Pain Assessment in Cancer Patients. Palliative Medicine : A Multiprofessional Journal **24**(4) (2010)
15. Jaquith, A., Balaouras, S., Schadler, T., Gray, B., Coit, L.: Apple's iPhone And iPad: Secure Enough For Business? (August 2010) `http://www.utahta.wikispaces.net/file/view/apples_iphone_and_ipad_secure_enough_for.pdf`.
16. Souppaya, M., Scarfone, K.: Guidelines for Managing the Security of Mobile Devices in the Enterprise. NIST Special Publication 800-124
17. Zhou, Y., Jiang, X.: Dissecting android malware: Characterization and evolution. In: Security and Privacy (SP), 2012 IEEE Symposium on. (May 2012) 95–109
18. Felt, A.P., Finifter, M., Chin, E., Hanna, S., Wagner, D.: A survey of mobile malware in the wild. In: Proceedings of the 1st ACM Workshop on Security and Privacy in Smartphones and Mobile Devices. SPSM '11, New York, NY, USA, ACM (2011) 3–14
19. Jaatun, M.G., Tøndel, I.A., Køien, G.M.: GPRS Security for Smart Meters. In Cuzzocrea, A., Kittl, C., Simos, D., Weippl, E., Xu, L., eds.: Availability, Reliability, and Security in Information Systems and HCI. Volume 8127 of Lecture Notes in Computer Science. Springer Berlin Heidelberg (2013) 195–207
20. Codenomicon: Heartbleed bug. http://heartbleed.com (April 2014)