Satisfaction of Health Record Security Principles through Collaborative Protocols

Salem Aljareh and John Dobson
School of Computing Science, Newcastle University, UK
Nick Rossiter
School of Computing Science, Northumbria University, UK

Abstract. The general nature of security requirements in health care systems is described. The CTCP/CTRP model, designed for handling these requirements and developed in earlier work, is introduced. This model covers requirements, policy and materials and is represented by two protocols: CTCP the Collaborative Task creation Protocol and CTRP the Collborative Task Runtime Protocol. The principles of two British approaches (DPA and Caldicott) are presented and it is shown how these are handled by the CTCP/CTRP model.

Introduction

In business-oriented information systems, requirements are determined by interviewing a single client. For instance techniques such as OMNIS [8] have been particularly designed for handling the documentation and analysis of such user requirement. Fundamentally, requirements come into view as a result of the observation of existing systems along with information on how to improve, add more functions/services or maybe change to a better situation.

For requirements in general including those for security, the first stage of requirements is often rhetoric, such as a complaint about services, a request for new services or an invitation to react to environment changes or new regulations. The second stage of the requirements takes the form of statements/principles. These statements or principles aim to predicate the general requirements in rhetoric and make them more specific and appropriate for further developments.

In security systems the general rhetoric aims to achieve the three main aspects of security: confidentiality, integrity and availability. In some literature accountability is counted as a fourth aspect. However accountability is not an objective in its own right. Indeed it is more a mechanism that exists to help ensure the other aspects are satisfied. Rhetoric in this case is regularly expressed as general security statements formally called a security policy or security regulation depending on the application. There could also be concerns about existing threats to the system.

The concept stage in security requirements could be security principles, security policy models or any revised version of security statements such as official rules and regulations of an organization, ethical codes in a moral network and beliefs of an individual or group. Ross Anderson [4] illustrates general definitions, worth mentioning, for the security policy models along with some examples including his model for the British Medical Association (BMA).

Confidentiality: (patient's right requirements)

With respect to the patient's rights, recent legalisations and publication in the field support five important aspects:

1. Patient oriented approach: an item of information about a patient should be owned by the patient described by the information.
2. Privacy: patient privacy should be maintained to a high standard as a result of fair and lawful use of the patient's confidential information.
3. Transparency: the patient should be made aware of all the use made of his information.
4. Public interest: the need of the community may override the need of individuals in some exceptional cases.
5. Legal requirements: a trial case may require disclosure of a patient's confidential information. However this should be very restricted and limited by the case after detailed explanations of why the information disclosure is essential.

Concept

There are a number of official statements and principles from which security requirements for health information systems can be derived. All of these principles aim to protect the patient's sensitive information, particularly person-identifiable information based on the patient's rights. However it has been understood that some of these principles result in much debate and conflict [3, 7]. As a result an implementation of this requirement is a difficult task. There are two general, equally rated, goals for health care services: a good quality of health provision (not only for a certain patient but for all of society e.g. the requirements of medical research)

and full respect for the patient rights. In this work we will look at two accepted approaches: the Data Protection Act and the Caldicott Principles and recommendations. These two approaches are both relevant to security in health care services. The Data Protection Act is the general law of Britain for controlling the use of personal data and the Caldicott Principles are an attempt to develop a specific means of controlling access to personal information in health services in the context of general British law and the culture of the health services. Both of the documents underpinning the approaches give lists of principles.

The CTCP/CTRP Model

The full details of the model are given elsewhere [1, 2]. The main component in our CTCP/CTRP (figure 1) is the collaborators (two or more), each of which will need to define three elements: requirements (what does he/she/it/they aim to gain from the other side), policy (rules that need to be obeyed) and material (e.g. information to release or services to offer). The second component is a pair of task-based collaboration protocols -- the Collaboration Task Creation Protocol (CTCP) and the Collaboration Task Runtime Protocol (CTRP), both detailed in [1, 2]. CTCP includes a negotiation between all collaborators where the proposed task will be discussed including all collaborators' policies and requirements. This process (negotiation) continues until a decision is taken either by rejecting the proposal or by accepting it. The acceptance of a proposal will lead to a formal agreement/contract, which will produce the proposed collaboration task in its final stage including all of the policies and requirements. CTRP will start after a successful compilation of CTCP and as scheduled in the *task_policy* (not necessarily immediately after the end of CTCP).

The main function of CTRP is to process the task that was previously created by the CTCP protocol and ensure that the *task_policy* is obeyed, that the collaborators are aware of the circumstances and that the right action is taken. In a special case of the abnormal termination of the task process the collaborators may need to go back to the CTCP protocol to create an alternative task. It should be noted that the *task_participants* (collaborators) are not necessarily the same subjects who were participating in the CTCP. However such features should be included in the *task_policy.* The case of an emergency update for the participants list during the CTRP will be covered by the CTRP process documentation (the CTRP log).

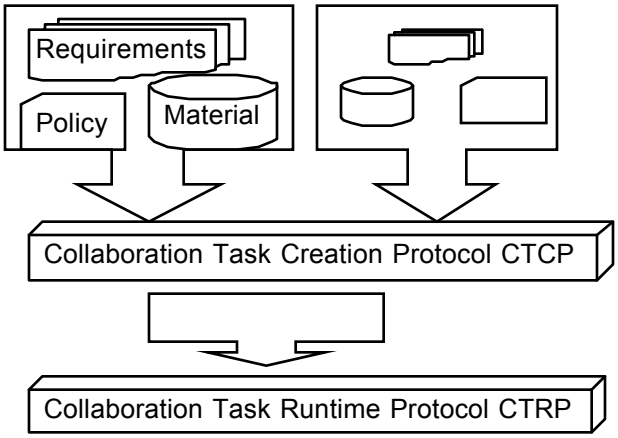

Figure 1: general architecture for secure collaboration environment

Data Protection Act

The Data Protection Act (DPA) [9, 10] is an implementation of the EC Directive 95/46/EC, which aims to protect the processing of personal information by 'data controllers'.
The DPA has been summarised into eight principles, which are discussed in the following paragraph with an attempt to examine how far these principles can be reflected in our CTCP/CTRP model:

Principle 1: *Personal data shall be processed fairly and lawfully.*

In our model sensitive data including personal data will be processed through a pre-defined task. This task is defined and created as a result of a collaboration protocol which in one of its steps involves negotiation between all parties, such as data subject (patient in EHR), service providers (who needs the information e.g. clinician, social worker), referee (optional, e.g. data controller) and legal agent.

Principle 2: *Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.*

By restricting the use of data by a specific task so that it can be used only for one purpose, so we can ensure that the data will not be used for more than one purpose.

Principle 3: *Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.*

The collaboration task will not be created unless the data subject and the referee (if any) make sure that this task will definitely need the required data.

Principle 4: *Personal data shall be accurate and, where necessary, kept up to date.*

Since the data subject is personally involved in the team that creates the collaboration task, so the personal data can easily be verified and updated.

Principle 5: *Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.*

In the CTCP protocol the start and the end date and time of a task should be explicitly specified and included in the *task-policy*. The CTRP protocol will ensure that all the task's activities will be processed within the specified time.

Principle 6: *Personal data shall be processed in accordance with the rights of data subjects under this Act.*

In our model we consider a data subject (patient in EHR) to act as the only owner for his/her personal information and he/she will never loss his ownership.

Principle 7: *Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.*

The task should be protected by law and by the available security mechanisms. In the CTCP firstly, at the *introduction* level there should be a proposal for the protection mechanisms/measures (including technical and legal aspects such as cryptography applications and prosecution) that can be used to protect a specific task that is going to use the patient information. If for any reason this proposal does not meet the security requirements then the task should be dismissed. At the *negotiation* level such mechanisms will be verified and tested and the task discarded if these mechanisms fail the test. All these mechanisms, after it has been found that they can do the job, will be encapsulated in the created task.

Principle 8: *Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.*

The data transfer task is a collaboration task that can be created using the CTCP/CTRP model. The data transfer will be allowed only among the collaborators who agreed in the CTCP protocol to adhere to each other's policies, which can include the protection for the rights and freedoms of data subjects in relation to the processing of personal data. The personal data will not only be protected against transfer abroad, it will also not be possible to transfer the data outside the task.

Caldicott Principles and Recommendations

In 1997-98 a committee chaired by Professor Caldicott at Cambridge developed security principles for the medical area [6]. The principles developed are an expansion and refinement of those found in the Data Protection Act. The emphasis is on control over the use of patient-identifiable information and the restriction of access to those who need to know information for particular purposes.

Principle 1: *Justify the purpose(s)*

This principle is right at the heart of our CTCP/CTRP model. In the CTCP protocol only one task will be created for each purpose. Later the extent to which the task adheres to the original purpose will be fairly tested and verified through the CTRP protocol.

Principle 2: *Don't use person-identifiable information unless it is absolutely necessary*

This principle can be easily achieved at the early stages in the CTCP protocol (*introduction*), where a good reason must be given to create a task. If for any reason the task does not need to use personal information, this task will simply be discarded either at the introduction or the negotiation stage.

Principle 3: *Use the minimum necessary person-identifiable information*

This is quite similar to the above Principle 2. In addition if it is found, in the process of the CTRP protocol (task assessment stage), that the task is using unnecessary information then the CTRP will be either aborted or updated.

Principle 4: *Access to person-identifiable information should be on a strict need-to-know basis.*

In our model the use of any material (person-identifiable information in this case) will be only through the task-participants. They are the only people authorised to use the information necessary

to perform the defined task. The task will be for only one purpose.

Principle 5: *Everyone with access to person-identifiable information should be aware of their responsibilities*

One of the main principles of our model is to clearly define the responsibility of all the task-participants before creating a task. Responsibility is declared at the negotiation stage in the CTCP protocol and evaluated at the task process assessment at the CTRP protocol.

Principle 6: *Understand and comply with the law. Every use of person-identifiable information must be lawful.*

This *someone* could participate at the agreement stage in the CTCP to prove or deny the tasks in which the use of the person-identifiable information appeared to be illegal. In addition at the stage of task process assessment in the CTRP this *someone* could monitor the task run and terminate it or update it if it is found to not comply with the task policy (either automatically or manually).

Coverage of Data Protection Act and Caldicott Principles

Not all the DPA principles, for instance 4,5,6 and 8, are covered by Caldicott. Principle 4, accuracy and timeliness of data, is assumed in medical data. Principle 5, length of time data is kept, does not apply to medical data as normally such data is kept while the patient is alive and longer if it can be used for tracing medical history for community or a family. Principle 6, rights of data subjects, is within the context of the DPA only. Principle 8, transfer of personal data abroad, is not covered by Caldicott because the data is considered to be anonymous anyway. Overall, the main concern in Caldicott is with protecting the assignment of data to specific persons. The BMA model [5] corresponds more closely to DPA than Caldicott.

From the other perspective, the Caldicott principles 2 and 4 are not reflected in the DPA. Both these are task based illustrating the need-to-know approach in Caldicott in contrast to the patient consent approach of DPA and BMA.

Review of Satisfaction of Principles by CTCP/CTRP Model

To conclude a review is made to show the extent to which the CTCP/CTRP model covers the principles of DPA and Caldicott. The purpose of this review is to show succinctly firstly whether each principle is covered and secondly the extent to which the requirements of software engineering [11] are met by the CTCP/CTRP constructions. Ideally there should be a tick at least once for each principle for coverage, a clearly-defined single functionality for each protocol for maximal cohesion, an encapsulation of the protocols for loose coupling and an efficient execution of the protocols for low energy performance.

Figure 2 shows the correspondence between DPA principles and CTCP/CTRP components. The ticks are shown only when the principle is explicitly covered by the component at the intension level. Ticks are not shown where the activity might arise for a particular case or instance at the extension level but such activity is not compulsory at the rule-based or intension level. For instance agreement (Agr) is implicit in most components but is explicit in number 8 where personal data is transferred to another country.

The decision protocol (Dec) is also implicit in many components but is explicit only in Principle 2 where it is required that the data will be used only for a specific task. The component for preparation (Pre) is implicitly involved in CTRP but is not explicitly highlighted in the table as we deal with general principles. Similarly the component update (Upd) in CTRP is also a very general principle dependent only on a case and used in emergency. The component for creating the CTRP protocol (Cre) appears to be excessively employed. However it is a task performing a critical linking task between CTCP and CTRP.

Figure 3 shows the correspondence between Caldicott principles and CTCP/CTRP components. The pattern is different from that for the DPA as Caldicott is in general more task-based meaning that there is much more explicit mention in the principles of the components we have created in CTCP/CTRP. For instance in Caldicott, Principle 1 (justify the purpose) requires explicitly all the components of CTCP/CTRP. Principle 4 (need-to-know restriction on person-identifiable data) is tackled on a task-based approach using agreement (Agr), creation of CTRP (Cre) and process logging (Log). The DPA is task-based in Principle 2 (data for specified and lawful purpose) corresponding to Principle 1 in Caldicott.

Figures 2 and 3 show that all the principles of DPA and Caldicott are covered by CTCP/CTRP. Every principle is cross-checked positively with one or more components in the model. CTCP and CTRP also exhibit maximal cohesion as the activities performed by these protocols are clearly differentiated. Thus CTCP creates the task including negotiation and agreement and CTRP runs the task assisted against the agreed policy. There is loose coupling between CTCP and CTRP. CTRP is encapsulated: it can only be called after CTCP has

successfully concluded. CTRP can be aborted resulting in a new CTCP session being started but this is simply a normal return mechanism. The high-level rule-based nature of CTCP/CTRP ensures an economical performance. Thus the model meets the software engineering requirements given earlier.

Conclusion

The CTCP/CTRP model appears to meet the general requirements of security for health informatics as outlined by Caldicott and the DPA. In terms of coverage a match is made with both the more specific task-based approach of Caldicott and the more general DPA. An analysis of the usage of the components of CTCP/CTRP against the principles of Caldicott and DPA shows that, while coverage is achieved in both cases, a more natural match is made with Caldicott than with DPA because Caldicott is at a more specific level in dealing with the patient record than DPA. The software engineering principles of maximal cohesion, low coupling and efficient execution are met by CTCP/CTRP. From a computing science perspective, CTCP/CTRP appears to be an appropriate way forward for handling security principles as developed in Caldicott and DPA. The next stage is to develop a case study using real case requirements in health care to test the whole approach.

References

1. Aljareh, S. and Rossiter, N. Modelling Security in Multi-agency environment, Newcastle University, Newcastle upon Tyne, 2002.
2. Aljareh, S. and Rossiter, N., A Task-based Security Model to facilitate Collaboration in Trusted Multi-agency Networks. in *ACM SAC 2002 symposium on Applied Computing*, (Madrid, 2000), 744-749.
3. Anderson, R. Remarks on the Caldicott Report., 1998.
4. Anderson, R. *Security Engineering: a guide to building dependable distributed systems*. John Wiley, New York, 2001.
5. Anderson, R., A security Policy Model for clinical information systems. in *IEEE Symposium on Research in Security and Privacy, Research in Security and Privacy*, (1996), 30-43.
6. Caldicott Committee. The Caldicott Committee Report on the review of patient-identifiable information, Department of Health, 1997.
7. Detmer, D. Counterpoint. Your privacy or your health - will medical privacy legislation stop quality health care? *International Journal for Quality in Health Care*, *12* (1).
8. Flynn, D.J. *Information Systems Requirements Determination and Analysis*. McGraw Hill Text, London, 1998.
9. Great Britain *Data Protection Act 1998 : Chapter 29.* Stationery Office, London, 1998.
10. Rosemary, J. *Data Protection Act 1998*. Sweet & Maxwell, London, 1999.
11. Sommerville, I. Software Engineering. Addison-Wesley, Harlow, England, 2001.

Principle	CTCP					CTRP						
	Int	Neg	Dec	Agr	Cre	Pre	Pro	Ass	Log	Upd	Dis	End
1	✔	✔	✔	✔	✔			✔	✔		✔	
2	✔											
3	✔	✔			✔			✔	✔		✔	
4				✔	✔			✔	✔			
5				✔	✔			✔	✔			
6				✔	✔			✔	✔			

Figure 2: Correspondence of DPA Principles and CTCP/CTRP Components

	CTCP					CTRP						
Principle	Int	Neg	Dec	Agr	Cre	Pre	Pro	Ass	Log	Upd	Dis	End
1	✔	✔										
2			✔	✔	✔			✔	✔			
3					✔							
4					✔							
5					✔							
6					✔			✔	✔		✔	
7					✔			✔	✔			
8	✔	✔		✔	✔			✔	✔			

Figure 3: Correspondence of Caldicott Principles and CTCP/CTRP Components