GEMSS: Privacy and security for a Medical Grid

Stuart E. Middleton[1], Jean A.M. Herveg[2], Federico Crazzolara[3], Darren Marvin[1], Y. Poullet[2]

[1]IT Innovation Centre, University of Southampton, UK
[2]Centre de Recherches Informatique & Droit, FUNDP, Belgium
[3]C&C Research Laboratories, NEC Europe Ltd., St. Augustin, Germany

Correspondence to:

Dr Stuart E. Middleton
IT Innovation Centre,
2 Venture Road
Chilworth Science Park
Southampton, UK, SO16 7NP
tel: +44 23 8076 0834
fax: +44 23 8076 0833
email: sem@it-innovation.soton.ac.uk

1. Summary

Objectives

The GEMSS project is developing a secure Grid infrastructure through which six medical simulations services can be invoked. We examine the legal and security framework within which GEMSS operates.

Methods

We provide a legal qualification to the operations performed upon patient data, in view of EU directive 95/46, when using medical applications on the GEMSS Grid. We identify appropriate measures to ensure security and describe the legal rationale behind our choice of security technology.

Results

Our legal analysis demonstrates there must be an identified controller (typically a hospital) of patient data. The controller must then choose a processor (in this context a Grid service provider) that provides sufficient guarantees with respect to the security of their technical and organizational data processing procedures. These guarantees must ensure a level of security appropriate to the risks, with due regard to the state of the art and the cost of their implementation.
Our security solutions are based on a public key infrastructure (PKI), transport level security and end-to-end security mechanisms in line with the web service (WS Security, WS Trust and SecureConversation) security specifications.

Conclusion

The GEMSS infrastructure ensures a degree of protection of patient data that is appropriate for the health care sector, and is in line with the European directives. We hope that GEMSS will become synonymous with high security data processing, providing a framework by which GEMSS service providers can provide the security guarantees required by hospitals with regard to the processing of patient data.

2. Keywords

Grid, Legal, Medical, Personal Data, Security

3. Introduction

The goal of the GEMSS project (Grid-enabled Medical Simulation Services) [12] is to develop a test-bed for six medical imaging applications. We use a client-server service-oriented architecture, where clients negotiate with a set of potential service providers, select the best candidate and securely submit a Grid job to that service provider. The chosen service provider runs the medical simulation and securely returns the results to the client, who pays for this service according to an agreed business model.

For example, a medical physicist working at a hospital in the UK might negotiate with a number of radio-surgery service providers around Europe, select a service provider in Germany and make a reservation on the German's computing cluster for the next week. The medical physicist would then book the patient in, perform a MRI scan of the patients head, create a treatment plan and submit this plan to the service provider. The service provider would then run the radio-surgery simulation service and return the resulting dosage profile to the medical physicist, who can make a judgement about the quality of the treatment plan.

The use of Grid technology in the healthcare sector raises significant legal and security issues. In this context, the GEMSS project examines explicitly both the legal and security framework in which such Grid tools could be exploited.

Our legal study analyses the pertinent European regulations concerning the six GEMSS medical simulation applications. This analysis allows us to draw up the common legal framework under which GEMSS applications can be developed in Europe. We also identify aspects not covered by European law, and where national laws might conflict. Considering the normative plurality characterizing the European legal system, the three viewpoints considered most relevant for this analysis are:

- Protection of privacy with regards to the processing of patient data.
- Contractual aspects.
- Responsibilities and liabilities concerning the use of GEMSS applications.

In this paper we give the legal qualification of the operations performed upon the patient's personal data, in view of Directive 95/46 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. We also identify the legal requirements resulting from this analysis.

Our security analysis looks at the security solutions available to the GEMSS project, both technical and procedural, and provides advice as to the methodology involved in assessing a specific site's security.

In this paper we present the security solutions chosen for the GEMSS infrastructure, and identify how these solutions match the identified legal requirements from our legal analysis. The basic security technology employed in GEMSS is based on a public key infrastructure (PKI), and implements end-to-end security mechanisms in line with the web service (WS Security, WS Trust and SecureConversation) security specifications.

We conclude with a short discussion of the progress so far, and shed some light on our ambitions for this work both within the GEMSS project and during the exploitation phase after the project completes.

4. Objectives of this paper

- Present our analysis of applicable EU law to the running of medical simulation services on a pan European Grid

- Summarize the legal requirements resulting from our analysis
- Describe the identified security solutions that fulfil these legal requirements
- Discuss progress so far and our ambitions for this work

5. Application of EU directive 95/46 to GEMSS applications

The EU Directive 95/46 must guide GEMSS applications since, according to its article 3.1, it applies to wholly or partly automated processing of personal data [2]. It also applies to other types of processing of personal data, which form a filing system.
In the context of Directive 95/46, the previous radio-surgery example application would contain a patient, some personal data (treatment plan derived from MRI images), a controller (UK hospital), a processor (German service provider) and an electronic register (Grid service registry).
Directive 95/46 make it clear that any patient data, send to the service provider via the internet as a treatment plan, is personal data since it is related to a well-identified natural person. If the data sent via the Internet is not directly nominative, but can via some code be attributable to an identified person, it is also personal data. The transmission via the Internet and subsequent processing by a service provider constitute sets of operations performed upon personal data by automated means.
It should be noted that the processing performed by a GEMSS service provider is only one part of the complete set of operations performed upon the patient's data, in order to support the healthcare provided to him by his medical practitioner. All the sets of operations performed upon the patient's personal data are integral parts of the same and unique data processing defined by its therapeutic purpose, and to which they are linked. This implies that the use of the GEMSS applications does not create a new processing of personal data. Their use is only a new part of a pre-existing processing of personal data for therapeutic purpose or for scientific research. If necessary, the controller of the personal data processing will have to adapt his procedures to the use of such new tools, according to the applicable national rules transposing directive 95/46.

6. Processing and sub-processing of the patient's data by a GEMSS service provider

When processing personal data on behalf of the controller, the GEMSS service provider acts as a processor defined in article 2, e, of Directive 95/46. The controller must thus choose a processor whom provides sufficient guarantees in respect of the technical and organizational measures governing the processing to be carried out, in accordance to article 17, § 2, of Directive 95/46. The controller must ensure compliance with those measures.
Providing software (i.e. software vendors) to help the imaging processing does not constitute in itself an operation performed upon personal data.
A processor must be governed by a contract or legal act binding the processor to the controller, and stipulating in particular that the processor shall act only on instruction from the controller. Such a contract should also stipulate that the appropriate technical and organizational measures, as defined by the law of the member state in which the processor is established, shall also be incumbent on the processor, according to article 17, § 3, of Directive 95/46. The parts of the contract relating to data protection shall be in a written form (or equivalent), according to article 17, § 4, of Directive 95/46.

7. Legal requirements deriving from legal analysis

The data controller and the GEMSS service providers have to protect personal data against accidental or unlawful destruction, alteration and loss etc. Both the controller

and processor must protect patient's data against unauthorized access or disclosure, in particular when the processing involves the transmission of data over a network, and against all other unlawful forms of processing. Table 1 summarises these legal requirements.
With regard to the state of the art and the cost of implementation, such measures have to ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected [3]. Consequently, the more sensitive the data is, the more risky the processing will be. As personal data related to health is very sensitive, the security level of the data processing has to be at maximum.
For examples of security measures, it is useful to refer to the measures recommended e.g. by Rec. 1997(5) of 13 Feb. 1997 of the Council of Europe on the protection of medical data, article 9 [4].

8. Security solutions within the GEMSS HealthGrid

The GEMSS Grid infrastructure is capable of providing a high degree of security for the processing of personal data. Our security mechanisms ensure the confidentiality and integrity of personal data, and that data processors are identified, authenticated and authorized. Our security solutions are based on a public key infrastructure, transport level security protocols and end to end security protocols. Along with an intrusion detection system these solutions provide GEMSS with security in depth. Table 1 shows how the legal requirements of the previous section relate to our security solutions, and figure 1 shows how our security is split between the client and server sides of the GEMSS architecture.
A public key infrastructure (PKI) uses certificates to identify parties, employing asymmetric public key encryption and a trusted third party to control certificate issue and revocation. Our public key infrastructure follows the guidelines defined in the X.509 Internet drafts and standards [5], [6], [7]. We have drafted a GEMSS certificate policy [8] and defined roles for the certification authority (CA), registration authority (RA) and relying party. Our certificate policy clearly defines procedures for requesting, issuing, revoking and distributing GEMSS certificates. All GEMSS certificates are in the X.509 certificate format [9] and are used by people or machines for authentication, identification and authorization purposes on the GEMSS Grid. The certificate policy and the certification practice statement of the GEMSS certificate authority ensure that the GEMSS certificates issued to people are in line with directive 1999/93EC of the European parliament and the council on a community framework for electronic signatures [10].
Transport level security involves the basic security and encryption mechanisms involved with transmitting data over the Internet. We authenticate our communication points using the HTTPS protocol, allowing our data to be transmitted confidentially and with integrity. Within the GEMSS Grid both the clients and service providers are protected by firewalls, and as such belong to different trust domains. We have also set-up intermediate demilitarized zones (DMZs) at our service provider's sites, which forward relevant messages to more protected internal network domains. Demilitarized zones provide a buffer zone, so should a hacker gain access to computers with public IP addresses they would still need to discover and access computers with private internal IP addresses.
End-to-end security protocols apply a security policy to ensure that the message originator is authenticated, that the message itself has not been tampered with and for mutual authentication. Our end-to-end security mechanisms are based on the Web-Service security specifications [11]. Messages that contain personal data are first

processed according to a security policy before they are handed over to the transport layer. In turn, when a message arrives, the transport layer hands the message over to a security module, which helps perform the necessary signature verification and decryption. These security modules sit at the communication end-points of both the GEMSS service provider and client, enabling better integration with health care security infrastructures. We secure end-to-end channels using security token services, whose security tokens are required by the security policy.

In GEMSS we also use certificates for authorizing access to selected GEMSS services and resources. The access rights associated with a certificate are assigned according to the applied business process, and enforced through a GEMSS service-level authorisation component.

It should be noted that, although the risk of intrusion and attack to the GEMSS Grid is minimised by our security mechanisms, it cannot be completely excluded. As such our infrastructure includes an intrusion detection system capable of detecting intrusions and attacks. The logs produced by this system can help detect security breaches, and might be used as forensic evidence for potential legal action against intruders.

9. Conclusions

GEMSS clients (e.g. hospitals) are controllers of the patient data. GEMSS service providers act as processors on behalf of the controller of the patient's data processing for healthcare purpose. With respect to this, the controller must choose a processor who will provide sufficient guarantees in respect of the technical and organizational measures governing the processing to be carried out. The controller is also responsible for ensuring processor compliance, and needs a written contract to accomplish this. The level of security required must be appropriate to the risks represented by the processing and the nature of the data, with due regard to the state of the art and the cost of implementation. Considering the very sensitive nature of the personal data related to health, the level of security for GEMSS has to be at maximum.

Within the GEMSS infrastructure there are several levels of protection, including a robust and standardized public key infrastructure, transport level security protocols and end-to-end security protocols. Our security solutions ensure the confidentiality and integrity of personal data, as well as authentication of the data processors. If our protection was broken, an additional logging and intrusion detection system provides security in depth. We hope that GEMSS will become synonymous with high-security personal data processing for the healthcare sector.

The immediate next steps for us in GEMSS is to finish reviewing EU contractual law and perform a review of commercially available off the shelf security tools. We have currently implemented the public key infrastructure and transport level security protocols, and are now working on the end-to-end security mechanisms and service-level authorization. Towards the end of the project we will be looking at HealthGrid liability issues and the security and legal needs during any exploitation phase after the project.

10. Acknowledgement

This work was supported by the EC under Research Contract IST-2001-37153 GEMSS (GRID-enabled Medical Simulation Services)

11. References

1. D. 95/46 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. O.J. 23/11/1995:L 281,0031-0050.
2. Herveg J, Poullet Y. Directive 95/46 and the use of GRID technologies in the healthcare sector : selected legal issues. Proceedings of the 1st European HealthGRID Conference, Lyon, January 2003; 229-236.
3. Article 17, § 1, of Directive 95/46.
4. Cf. also: http://europa.eu.int/comm/internal_market/privacy/workingroup_en.htm.
5. Information technology – Open Systems Interconnection – The Directory: Authentication Framework. ITU-T Recommendation X.509, ISO/IEC 9594-8, March 2000.
6. Arsenault A, Turner S. Internet X.509 Public Key Infrastructure: Roadmap. Internet Draft, PKIX Working Group, July 2002.
7. Chokhani S, Ford W, Sabett R, Merrill C, Wu S. Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework. Internet Draft, PKIX Working Group, April 2003.
8. Crazzolara F. GEMSS Certificate Policy, v 1.0, September 2003.
9. Information technology – Open Systems Interconnection – The Directory: Authentication Framework. ITU-T Recommendation X.509, ISO/IEC 9594-8, March 2000.
10. D. 1999/93 on a Community Framework for Electronic Signatures. O.J. 19/01/2000 : L013, 0012-0020.
11. Security in a Web Services World: A Proposed Architecture and Roadmap. IBM Corporation and Microsoft Corporation – joint security whitepaper, Version 1.0, April 2002.
12. GEMSS public home page: http://www.ccrl-nece.de/gemss/

12. Figures

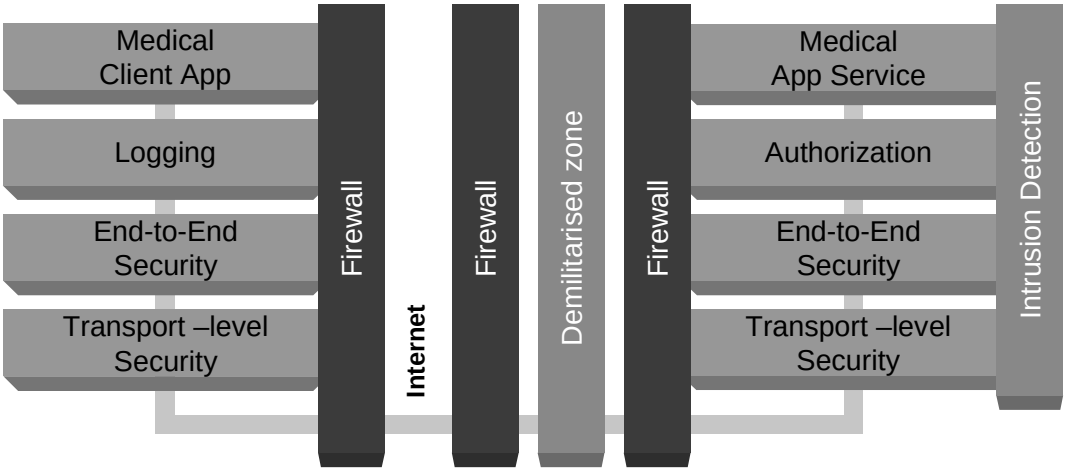

Fig. 1 : Overview of the GEMSS security infrastructure

13. Tables

Table 1 : Legal requirements and security solutions used in GEMSS

Legal requirement	***Security solutions***
Protect	
Data in transit	PKI, X.509 compliance, WS Security, HTTPS
Prevent	
Accidental and unlawful loss of data	PKI, certificate access rights
Unauthorized access to data	Firewalls, access control
Unlawful processing of data	PKI, WS Security, Intrusion detection, logging

14. Summary

Objectives

The GEMSS project is developing a secure Grid infrastructure through which six medical simulations services can be invoked. We examine the legal and security framework within which GEMSS operates.

Methods

We provide a legal qualification to the operations performed upon patient data, in view of EU directive 95/46, when using medical applications on the GEMSS Grid. We identify appropriate measures to ensure security and describe the legal rationale behind our choice of security technology.

Results

Our legal analysis demonstrates there must be an identified controller (typically a hospital) of patient data. The controller must then choose a processor (in this context a Grid service provider) that provides sufficient guarantees with respect to the security of their technical and organizational data processing procedures. These guarantees must ensure a level of security appropriate to the risks, with due regard to the state of the art and the cost of their implementation.
Our security solutions are based on a public key infrastructure (PKI), transport level security and end-to-end security mechanisms in line with the web service (WS Security, WS Trust and SecureConversation) security specifications.

Conclusion

The GEMSS infrastructure ensures a degree of protection of patient data that is appropriate for the health care sector, and is in line with the European directives. We hope that GEMSS will become synonymous with high security data processing, providing a framework by which GEMSS service providers can provide the security guarantees required by hospitals with regard to the processing of patient data.

15. Keywords

Grid, Legal, Medical, Personal Data, Security