NeuroLOG ANR-06-TLOG-024
Software technologies for integration of process, data and knowledge in medical imaging

Financé par ANR

Deliverable L10:

Security policies set-up

Authors : Alban Gaignard
Johan Montagnat
David Godard

Summary: This document summarizes the security constraints identified in the context of the NeuroLOG project and the solutions implemented in the NeuroLOG middleware. The security policies designed and described in this document are implemented and integrated in the prototype plateform currently deployed.

Document layout

1. Summary of requirements

The security requirements arising from the NeuroLOG end users have been detailed in an internal project document [1]. This section only provides a brief summary of the requirements identified.

1.1. Data distribution and security

The NeuroLOG platform is distributed and as such expose data sets and user activities over the Wide Area Network. All data manipulated and all user activities need to be protected from unsolicited observation.

1.2. Authentication

All platform users need to be properly identified and their activity relating to the manipulation of sensitive resources traced.

The most sensitive resources handled by the NeuroLOG middleware are image files and application processing tools. The image files contain private patient information and is often considered as a valuable resource belonging to the radiology center that performed the image acquisition. Some image processing tools are research tools that are not intended for public use until they have been properly validated and exploited by their authors.

In a neurology community such as the one using the NeuroLOG middleware, the metadata associated to the patient image files is not very sensitive given that (i) it has necessarily been anonimized prior to exploitation for research and (ii) it has no value independently from the image files it describes. Hence, metadata and semantic data is not considered as critical.

In the requirements analysis document [1], there is a proposal for anonimizing and encrypting data stored locally within each site. It appeared that this functionality is not achievable in the context of the NeuroLOG middleware. Indeed, the middleware provides a federation layer for data sets that are imported externally to the NeuroLOG platform. The middleware has no control on the data integration phase where such operations should be performed. It has therefore not be considered.

1.3. Authorization

The authorization framework applies to image files and image processing tools. It needs to accommodate to two partly conflicting requirements: the need for sharing data sets among sites and the desire of each site to solely control access to the data it owns. A specific security policy has been designed to achieve a trade-off between sites autonomy and data federation.

2. Middleware security layer

Security is the bottommost layer of the NeuroLOG middleware. It strongly influenced the technological choices made and it was integrated very early in the software integration process in order to validate the security technologies

considered. The security is based on standard X509 public certificate / private key pairs for identification of system users. A certification authority deployed specifically for the NeuroLOG federation issues certificates. Trust certification chains are established between sites participating to the federation and all communications between sites are secured over the SSL transport layer. The middleware is designed as a set of inter-operating web services. The SSL layer protects all SOAP messages that are used for communication between Web Services (use of the HTTPS protocol). File transfer are either achieved through Web Service streaming (MTOM protocol), therefore benefiting from SSL protection or directly though HTTPS.

In addition to data protection, the middleware provides access control to complete system security, as described in the next section.

3. Security policies designed

A strategy for implementing a suitable security policy has been described in an internal project document [2] and recently published at the HealthGrid'09 conference [3]. This section only provides a summary of these documents.

3.1. Security policies

A centralized access control solution is not acceptable as no clinical site would accept access control on its data to be performed externally and the notion of federation wide super user cannot be implemented. The NeuroLOG middleware needs to address access control over data sources distributed over a federation where each site implements a singular local policy. It has to support multi-centric studies involving data sharing, yet preserving autonomous sites administration.

The NeuroLOG access control mechanism is based on traditional Role-Based Access Control (RBAC). RBAC assigns permissions to roles (the user possible functions) in such a way that access control policies remain light and easy to understand. Most existing RBAC systems are centralized and they manage two different functions simultaneously: (i) the assignment of roles to users and (ii) the definition of access rights for each role. The NeuroLOG system decouples these two functions to achieve distributed access control with prevailing local policies.

On each site, at least one administrator has privileges to register the site users and to maintain the site's access control policy. Users may belong to different trust domains (a system administrator usually has no complete view of the potential users of the system) while the access rights to data of a given domain has to be ultimately controlled by this domain's administrator. The compromise to enable collaborative work while ensuring site-wise access control to local data is as follows:

- Site administrators are capable of creating federation-wide roles, as many as needed to describe their access control policies;
- The creator of a role controls the assignment of all system users to that role: the management of a particular role is centralized on one of the sites.

- Each site administrator controls the assignment of federation-wide roles to permissions related to their local resources.

A user is granted access to a data item if she belongs to at least one role that is locally authorized to access this item. This policy framework ensures that sites solely control access to their data: only a site administrator can bind some role to her data. It also ensures that each role is well defined and administrated: only the role creator can bind users to that role. It implies collaboration between the data owner and the role creator: the data owner agrees to make some data accessible for a particular role (*e.g.* in the context of a particular multi-centric study); the role administrator is trusted and recognized as the administrator for this particular study. Any user in the federation can collaborate to the study: through the certification chains, the role administrator can validate the identity of any user before assigning the role to her. Finally, the roles are guaranteed to be unique federation-wide through the Federation Registry. Roles can only be created after assignment of a unique name through the unique Registry.

This system is agile and preserves sites autonomy: sites are only tightly coupled to the Registry and they do not depend on it for their normal operation. The authorization scheme is lightweight and can quickly dynamically evolve to adapt to new needs for collaborative studies.

3.2. Middleware integration

The same NeuroLOG security policy is implemented both for data and processing tools access control. The mechanism to enforce access control differs in each case though. Data can only be accessed through NeuroLOG middleware services: it is therefore the responsibility of the internal data manager to perform control on each data access. Image processing tools are exposed as regular web services hosted in a web service container (Tomcat) on each site. In that case, services need to be instrumented to enforce access control on each invocation of the tool. This is achieved through the jGASW service wrapper implemented in the context of the project: jGASW generates a Web Service interface to application services together with extra code for performing access control on the fly.

4. System activity traces

The sensitive actions traced by the system are:

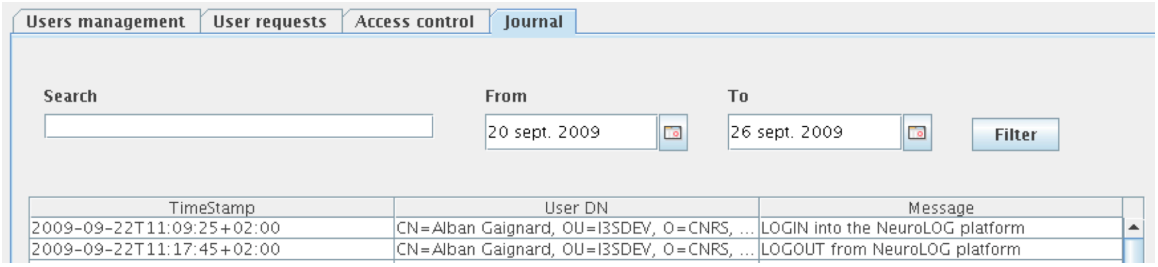
- User login and logout
- File access attempts
- Processing tools access attempts

All traces are recorded on the site that is impacted by the access for coherency and non-repudiability: users login/logout are recorded on the site users are registered in, file accesses are recorded on the site that published them, and processing tool accesses are recorded on the site that deployed them. Traces are made persistent by recording in a database.

A system activity trace is constructed with (i) a time-stamp, (ii) the DN of the user and (iii) a text message describing the action performed by the user. The

time-stamp is generated from the time clock of the server that receives a request. The DN of the user corresponds to the «Distinguished Name» of it's personal X509 certificate and is automatically retrieved by the application container from the SSL communication layer. Finally a human-readable message is constructed to describe the type of user action and eventually the resource access attempt.

A graphical user interface dedicated to site administrators has been developed. It allows the visualization of the site activity through traces stored on each local administrative database. By default, all traces of the current week are displayed. Administrators can filter traces by defining start/end dates or by defining in the search filter a text that should be present, either in the DN column, or in the Message column. The following screenshot illustrates the graphical interface:



5. Perspectives

In order to simplify clinical end users authentication, we propose to implement single sign-on based on the healthcare provider or CPS (*Carte du Professionel de Santé*). The CPS is a smartcard used by French healthcare professional (physician, nurse, secretary, clinical researcher…) in order to:

- identify them regarding to Health Information System and medical software, and
- identify them and secure exchange with French social insurance.

The "Groupement d'Intérêt Public Carte de Professionnel de Santé" (GIP-CPS) is responsible for defining the CPS card and the read device (Heterogeneous environment: Windows, Mac Os X, Linux), for developing the CPS card, for issuing and managing it and for promoting the whole CPS system to the Application Providers and to the Healthcare Providers.

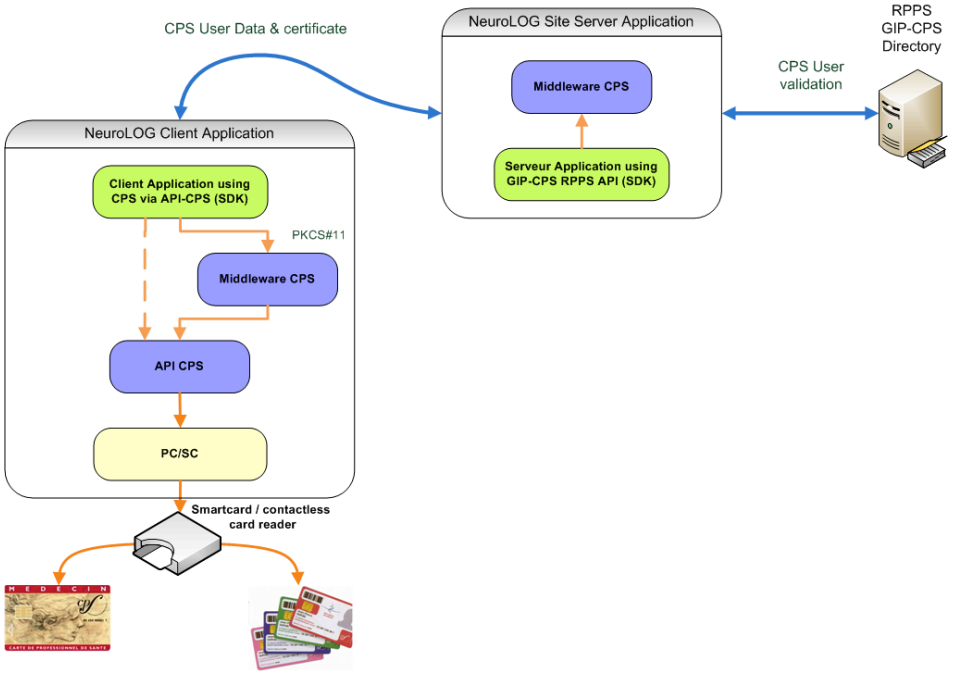
GIP-CPS provides Software Development Kit (SDK) to software manufacturers [4], acts as a Certificate Authority and provides a centralized health professional directory ("Le Répertoire Partagé des Professionnels de Santé" or RPPS).

Each medical user has a CPS card that contains her nominatives information and her X.509 certificate. This certificate enables to validate the user identity by querying the GIP-CPS authority and is used in all communication security mechanisms (data signature, communication encryption…) provided by the SDK.

Today GIP-CPS SDK can manage two kinds of CPS card:

- CPS2Ter, a smartcard like bank card,
- CPS3, a third generation card that can act as CPS2Ter smartcard but also as a contactless card. CPS3 will start to take office on Q4 2009.

We propose to support at least the CPS2Ter in our security policy following the next schema:



- Using CPS SDK, the NeuroLOG client application can get user information and certificate read from the CPS card,
- This data is transmitted to NeuroLOG Site server,
- The NeuroLOG server has an authorized access to RPPS GIP-CPS Directory and it can query the directory to validate the user identity.

6. Bibliography

[1] A. Gaignard, J. Montagnat, “NeuroLOG Security Requirements”.

[2] J. Montagnat, D. Godard. “NeuroLOG Security Policy proposal”.

[3] A. Gaignard, J. Montagnat. "A distributed security policy for neuroradiological data sharing" in Proceedings of the HealthGrid'09, pages 257-262, IOS Press, Berlin, Germany, June 2009.

[4] L'espace éditeurs du Groupement d'Intérêt Public - Carte de Professionnel de Santé. https://editeurs.gip-cps.fr/.