Allée de la Réflexion

L'évolution des normes de sécurité…

…vers plus d'auditabilité des systèmes d'information

Cet article présente les principales caractéristiques des aspects passés, présents et futurs de l'activité de normalisation et standardisation en matière de Sécurité des Systèmes d'Information de Santé.

Après un indispensable historique des diverses définitions de « sécurité » (I.T. security, sécurité des systèmes d'information et sécurité des systèmes d'information de santé), nous aborderons la distinction entre la standardisation « de facto » du passé et celle « de jure » du présent et du futur. Nous insisterons sur les aspects primordiaux des activités de la sécurité des systèmes d'information de santé, fondés sur le fait que ces systèmes exigent des normes et standards de sécurité particuliers. Pour être pertinent il est nécessaire de faire une distinction entre sécurité et qualité, entre sécurité-'security' et sécurité-'safety', entre sécurité et intimité, entre confidentialité-discrétion et confidentialité-séclusion (anonymisation ou pseudonymisation) et enfin entre auditabilité et 'accountability'.

En conclusion, nous rappellerons que la normalisation n'est pas seulement une affaire d'experts mais aussi et, en priorité, le résultat des exigences des acteurs du secteur. Nous montrerons que l'auditabilité est la propriété d'avenir des systèmes d'information de santé (médicaux et hospitaliers) pour accroître la confiance à placer dans la sécurité de ces systèmes pour une meilleure qualité des systèmes eux-mêmes.

Préambule (introduction)

Le contexte

Le colloque « Présent et avenir des Systèmes d'Information et Communication Hospitaliers (SICH) » organisé à l'Hôpital Européen Georges Pompidou (HEGP) aborde différents angles de vue notamment celui, transversal, de la sécurité des communications (cf. Session V : communication et sécurité).

Dans le cadre plus général de la sécurité, cet article traite de la sécurité des informations et des communications dans le contexte spécifique de la sphère santé, et dans l'environnement de l'informatique hospitalière. Il se focalise sur le « présent et l'avenir de la normalisation en informatique de santé ».

Notre propos n'est pas de passer en revue l'ensemble des normes en vigueur, en cours d'élaboration, ou en projet, dans le domaine de la sécurité des systèmes d'information de santé. Un long article ne suffirait pas à commenter les aspects conceptuels et techniques d'une seule de ces normes.

Pour une bonne compréhensibilité et ainsi une meilleure appropriation des informations, en particulier par un lecteur néophyte, nous nous limiterons (ce qui résume malgré tout quelques années.hommes d'activité en normalisation) à :

- un bref rappel des documents normatifs de référence en sécurité de manière générale : ISO 7498-2 [1], TCSEC [2], ITSEC [3], Common Criteria [4], ISO 17799 [5], GMITS 1-5 [6], ISO 10181 1-7 [7] ;
- un rapide survol des normes de sécurité tant génériques que sectorielles : ENV 12251 :2000 [8], ENV 13729 :1999 [9], ISO 17090 [10], CR 13694 :2000 [11] ;
- un parcours plus détaillé des principales normes de sécurité dédiées à la sphère santé : ENV 12924 [12], ENV 13606-3 [13], ENV 13608-1 [14], FD S 97-560 [15].

Les normes ou documents normatifs relatifs à la sécurité dans la santé, commentés plus en détail dans cet article, sont issus de trois groupes et niveaux de normalisation auxquels la France participe activement :

- national : le groupe GE-SSIS[1] au sein de la CNIS[2] d'AFNOR[3] ;
- européen : le groupe WG III[4] au sein du TC251[5] du CEN[6] ;
- mondial : les groupes WG 4 et WG 5[7] au sein du TC215[8] de l'ISO[9].

Présentation de l'article

Cet article se propose de faire découvrir au lecteur non initié, l'existence des nombreux travaux de normalisation effectués ou projetés en informatique de santé. Cet article montre l'ampleur et la nécessité de poursuivre ceux qui la sécurité de ces systèmes d'information de santé ; ces travaux sont complémentaires de ceux menés autour de la sécurité des systèmes d'information en globalité.

Notre exposé, en parcourant les normes les plus représentatives de l'évolution de la sécurité informatique, présentera :

- la progression de la perception de la sécurité depuis la sécurité originelle des systèmes d'exploitation, en passant par la sécurité classique des systèmes informatiques, jusqu'à la sécurité actuelle des systèmes d'information du secteur santé, voire hospitalier ;
- l'apparition des tendances actuelles et futures en matière de besoins de sécurité, plus particulièrement spécifiques à la sphère santé/social et au secteur l'hospitalier ;
- l'orientation des futures architectures de sécurité à construire pour prendre en compte ces nouveaux besoins et répondre aux questions liées aux développements des nouvelles technologies de l'information et de la communication.

La composition de cet article est la suivante :

- un historique de la définition de la sécurité (matériel) ;
- les relations entre la sécurité et la normalisation (méthode) ;
- l'évolution dans la prise en compte de normes (résultat) ;
- les tendances actuelles et à venir en sécurité (discussion) ;
- les enseignements pour la sécurité de demain (conclusion).

Histoires de la sécurité (matériel)

Ce chapitre est un préalable nécessaire à une meilleure compréhension de l'évolution de la notion de sécurité – informatique à l'origine et désormais appelée des systèmes d'information – c'est-à-dire de la progression de la perception qu'ont de la sécurité les différents acteurs des systèmes d'information.

Nous verrons que la sécurité, toujours destinée à éviter les malveillances, a progressivement étendu son champ d'investigations et son spectre de besoins, depuis le strict contrôle d'accès de bas niveau, jusqu'aux garanties juridiques de bon fonctionnement.

---

1 *GE-SSIS : Groupe d'Experts en « Sécurité des Systèmes d'Information de Santé » de la CNIS.*
2 *CNIS : Commission de Normalisation "Informations de Santé" d'AFNOR.*
3 *AFNOR : Association Française de NORmalisation.*
4 *WG-III : Working Group on "Security, Safety and Quality" du TC251.*
5 *TC251 : Technical Committee on "Health Informatics" du CEN.*
6 *CEN : Comité Européen de Normalisation.*
7 *WG 4 et 5 : Working Group 4 on "Security" et Working Group 5 on "Health Cards" du TC215.*
8 *TC215 : Technical Committee on "Health Informatics" de l'ISO.*
9 *ISO : Organisation Internationale de Standardisation.*

Sécurité informatique

La « sécurité informatique » dont on peut fixer l'émergence lors des années 70, est issue de travaux menés autour de la protection des systèmes d'exploitation.

Les systèmes « Multics » (cf. les anneaux) et « Unix » (droits d'accès), gèrent les conditions d'accès aux ressources de la machine et les droits d'accès aux fichiers (cf. « rwe » - read write execute). Ce sont les principales mesures de sécurité dites « logiques ».

Ces standards de facto (qui ne sont pas encore des normes de jure) utilisés par les principaux constructeurs d'ordinateurs, ont marqué cette première période.

On peut caractériser cette ère de la sécurité informatique par la notion de politiques de contrôle des droits d'accès : ainsi, se sont développées les deux premières catégories de politiques de contrôle :

- « par mandat » ou « obligatoires » (cf. 'MAC: Mandatory Access Control') ;
- « discrétionnaires » (cf. 'DAC: Discretionary Access Control').

Sécurité des technologies de l'information

La « sécurité des technologies de l'information », terme apparu lors des années 80, correspond à la prise en compte d'un ensemble plus large de contraintes, de problèmes, de risques et de solutions, pour développer la sécurité des technologies de l'information, ou « I.T. Security: Information Technology Security ». ISO 7498-2 [1] première norme internationale, calquée sur le modèle ISO/OSI est fondatrice de la sécurité ; lui ont succédé une série de documents, à caractère normatif, élaborés depuis les années 80 pour permettre d'évaluer la sécurité des systèmes :

- d'abord les TCSEC – Trusted Computer Security Evaluation Criteria (Orange Book) –édictés aux États Unis et apparus comme les fondements de l'évaluation de la sécurité, surtout des systèmes d'exploitation (cf. [2]) ;
- puis les ITSEC – Information Technology Security Evaluation Criteria – édictés en Europe et concurrents plus pertinents pour l'évaluation de la sécurité des systèmes (cf. [3]) ;
- et enfin, après une transition par des critères fédéraux américains (Federal Criteria), les Common Criteria – Security Techniques Evaluation for I.T. Security – édictés de part et d'autre de l'Atlantique pour fournir une norme mondiale d'évaluation de la sécurité, la norme ISO 15408 (cf. [4]).

La sécurité est, alors, considérée comme un facteur de qualité des systèmes ; c'est un argument de qualité de service, notamment pour les communications, et aussi l'un des attributs perceptifs du concept de sûreté de fonctionnement. Sa définition se stabilise autour de trois propriétés fondamentales applicables tant aux informations manipulées par les systèmes qu'aux systèmes eux-mêmes à travers leurs services, programmes, protocoles et mécanismes ; il s'agit du DIC regroupant :

- la disponibilité : les informations sont rendues disponibles selon des autorisations définies par la politique de sécurité du système ;
- l'intégrité : les informations ne peuvent être modifiées que d'une façon explicitement autorisée par la politique de sécurité définie pour le système ;
- la confidentialité : les informations ne sont pas divulguées en dehors des autorisations formellement accordées par la politique de sécurité définie pour le système.

On peut résumer cette ère de la sécurité des technologies de l'information par les concepts de politique de disponibilité – intégrité - confidentialité et de politique d'évaluation - certification de la sécurité.

Sécurité des systèmes d'information

La notion de « sécurité des systèmes d'information » (proche de la définition précédente) est apparue lors des années 90, dans le souci de prendre en compte d'autres aspects que ceux strictement liés à la technologie de l'information. Ces aspects incluent la gestion de l'ensemble des facteurs qui contribuent à la mise en place de politiques de sécurité et les responsabilités qu'elles impliquent.

Les normes suivantes illustrent cette préoccupation de sécurité globale du système considéré :

- la norme ISO 17799 (issue de la British Standard 7799) désormais référence mondiale en matière de sécurité des systèmes d'information, au plan générique (cf. [5]) ;
- la série de normes ISO 13335, les GMITS, série de directives pour la gestion et l'administration de la sécurité (cf. [6]) ;
- la série de normes ISO/IEC 10181, cadre de l'ensemble des aspects de la sécurité concernant l'interconnexion de systèmes ouverts (cf. [7]).

La prise en compte des notions de responsabilité relative à la sécurité et les besoins d'auditabilité de systèmes et de leurs sécurités sont déjà présents de manière générique. Cependant, ils ne constituent pas encore explicitement une attente de premier niveau, au même titre que la disponibilité, l'intégrité ou la confidentialité.

On peut résumer cette ère de la sécurité des systèmes d'information par le concept de politique de gestion et de contrôle de la sécurité, précurseur de la préoccupation globale de qualité de confiance.

Sécurité des systèmes d'information de santé

La spécificité sectorielle de la « sécurité des systèmes d'information de santé » par rapport à la sécurité générique des systèmes d'information évoquée précédemment, apparaît dans les années 90.

En effet, la spécificité du secteur de la santé, et même de la sphère santé/sociale, conduit à proposer des systèmes d'information (et des sécurités associées) appropriés, dans la mesure où les informations manipulées concernent, principalement, des acteurs ayant à la fois un rôle passif et une responsabilité non formellement impliquée : ce sont les patients, les malades, les assurés sociaux.

Le patient, le malade ou l'assuré social n'avait pas eu, jusqu'à cette époque, réellement voix au chapitre dans la construction, la validation ou l'utilisation des systèmes d'information de santé. Dans la plupart des cas, les données le concernant étaient saisies, traitées, étudiées, mises en statistiques, sans que son avis ne puisse être entendu. Alors qu'il s'agissait de données le concernant (dites « à caractère personnel ») et d'informations relatives à sa situation sanitaire (dites « à caractère médical ») ou sociale.

Ainsi, les années 90 ont vu se développer des notions et des besoins de sécurité propres à la sphère santé/sociale en général, et, plus particulièrement, au secteur médical, ambulatoire comme hospitalier. Nous développerons ces notions et besoins dans la suite de notre propos, mais citons simplement et pour mémoire : la traçabilité et l'opposabilité des actions, l'anonymisation ou la pseudonymisation des identifiants, la responsabilité des acteurs du système et, d'une manière générale, l'auditabilité du système et de sa sécurité pour une meilleure qualité de la confiance.

Que ce soit au plan national (à l'AFNOR), européen (au CEN) ou mondial (à l'ISO), des travaux de référence ont été menés dans ce sens, comme par exemple :

- l'ENV 12251 traite de l'authentification par mot de passe (cf. [8]) ;
- l'ENV 13729 traite de l'authentification par carte à microprocesseur (cf. [9]) ;
- l'ISO WD 17090 aborde la problématique des infrastructures à clés publiques sous l'angle technique du monde de l'informatique de santé (cf. [10]) ;
- le CR 13694 est un recueil des normes en sécurité informatique (cf. 'security') ou en sûreté-innocuité (cf. 'safety') vu sous l'angle de la qualité des logiciels (cf. [11]) ;
- l'ENV12924 propose une catégorisation des systèmes d'information de santé selon les niveaux d'exigences de sécurité exprimés par les établissements de santé (cf. [12]) ;
- l'ENV13606-3 aborde la problématique de partage de l'information médicale dans le cadre du dossier de santé électronique communiquant (cf. [13]) ;
- l'ENV13608-1 traite de la sécurité des communications de santé aux plans conceptuel, déontologique et normatif, propres aux attentes sectorielles (cf. [14]) ;
- le FD S 97-560 offre une méthodologie sécurité complète (glossaire, méthode, analyse et techniques) consacrée aux techniques d'anonymisation (cf. [15]) ;
- le FD S 97-700 offre une terminologie sécurité complète (glossaire, définition, homonymes et synonymes) consacrée à la sécurité dans la santé (cf. [16]).

Parmi ces normes on distingue deux finalités disjointes qui permettent de :

- raffiner partiellement des normes de sécurité génériques existantes afin de sensibiliser les acteurs du secteur santé à des questions essentielles préalables à toute démarche sécurité intelligemment mise en œuvre ; citons, par exemple, l'authentification par mots de passe ou par cartes à microprocesseur, la certification de clés publiques et la dualité entre sécurité et innocuité (cf. [8], [9], [10] et [11]) ;
- dédier à la santé, des normes de sécurité, spécifiques pour apporter aux acteurs de la santé les éléments de réponse juridiques, organisationnels, conceptuels, méthodologiques et techniques ; de façon à traiter les problématiques particulières non résolues par les diverses normes de sécurité, génériques existantes (cf. [12], [13], [14], [15] et [16]).

Sous des appellations parfois distinctes (traçabilité, imputabilité, opposabilité, irréfutabilité, non-répudiabilité, responsabilité ou encore 'accountability') des normes abritent des concepts connexes ; certaines de ces normes développent cette quatrième propriété de base de la sécurité qu'est l'auditabilité, à la fois complémentaire et orthogonale à ses trois homologues : la disponibilité, l'intégrité et la confidentialité.

La propriété d'auditabilité est complémentaire car elle garantit la confiance dans les trois autres ; c'est une véritable sécurité de la sécurité. La démarche d'auditabilité permet d'attribuer aux systèmes auditables (et à leur sécurité) un certain niveau de confiance.

La propriété d'auditabilité est orthogonale car, contrairement aux trois autres, elle est applicable au système à tous les niveaux, depuis la plus petite parcelle d'information, jusqu'aux processus de plus haut niveau (organisationnels, juridiques, etc.) ; alors que les trois autres propriétés s'adressent de façon particulière, soit aux données de bas niveau, soit aux informations de plus haut niveau d'intégration voire aux processus purement informatiques.

Certaines normes présentées supra (cf. [12], [13], [14], [15] et [16]) abordent et prennent en compte aussi bien la problématique juridique des responsabilités que les problèmes techniques et organisationnels.

On peut, alors, résumer cette ère de la sécurité des systèmes d'information de santé par le concept de politique de sécurité juridico-technique. Cette politique prend en compte, à la fois, cette nouvelle dimension juridique (et donc éthique et déontologique) et la précédente dimension technique plus classique, qui recouvrait les aspects organisationnels et opérationnels de la sécurité.

Sécurité des systèmes d'information et de communication hospitaliers

La « sécurité des Systèmes d'Information et de Communication Hospitaliers (ou SICH) » est actuellement en plein essor avec le développement des réseaux ville-hôpital, la progression du dossier de santé électronique communicant, la volonté de modernisation de l'ensemble des Systèmes d'Information Hospitaliers (SIH) en coopération avec l'évolution de l'ensemble des Systèmes d'Information de Santé (SIS).

Les SICH ont le privilège de pouvoir hériter de l'ensemble des acquis obtenus à travers les diverses ères de la sécurité : sécurité informatique et des technologies de l'information, sécurité des systèmes d'information puis des systèmes d'information de santé.

À l'inverse, les SICH ont l'inconvénient majeur d'avoir l'obligation de respecter un « modèle de spécification et de fonctionnement de la sécurité » capable de prendre en compte l'ensemble des problématiques essentielles de la sécurité :

- combinant les considérations d'ordre à la fois du juridique et du technique ;
- concernant à la fois la disponibilité, l'intégrité et la confidentialité ;
- prenant en compte les rôles, fonctions, responsabilités et usages dans l'hôpital ;
- intégrant les dimensions locale (intranet) et globale (extranet) ;
- conciliant les métiers du soin (cf. innocuité) et ceux de la recherche (cf. sécurité) ;

Seule, une démarche rigoureuse et scientifique peut prétendre répondre à l'ensemble de ces exigences et à leur complexité ; il s'agit de l'activité de modélisation formelle des politiques de sécurité :

- on doit modéliser les situations réelles auxquelles seront confrontées les politiques de sécurité à définir et à mettre en place ; la modélisation analytique permet d'atteindre le système le plus pertinent et le plus réactif possible, alors que la méthode énumérative risque de ne pas être exhaustive et de ne pas pouvoir prendre en compte une situation réelle complexe ;
- dès qu'il s'agit de santé, donc d'innocuité, des préoccupations de fiabilité apparaissent ; elles peuvent être résolues par la modélisation formelle de scénarios, contextes, environnements… très souvent considérés comme n'offrant pas de perception fiable de la situation : des travaux français (cf. projet MP6) et européens (au CEN/TC251) sont en cours sur ces sujet.[10]

On peut résumer cette ère de la sécurité des systèmes d'information et de communication hospitaliers par la notion de modèles de politiques de sécurité, qui doivent à la fois :

- répondre aux situations courantes, habituelles et quotidiennes, qui nécessitent de respecter des besoins de sécurité - certes non négligeables et non triviaux - mais d'ordinaire facilement traités (exemple : « qui peut accéder à quoi ? ») ;
- résoudre des situations conflictuelles, inhabituelles et exceptionnelles, soulevant quelques dilemmes décisionnels ; il convient de lever impérativement ces dilemmes qui combinent 'sécurité-security' et 'sécurité-safety' (ou innocuité) en prenant en compte les responsabilités des décisions prises, en intégrant les codes d'éthique, en respectant la déontologie et les lois (exemple : en cas d'urgence et en l'absence de l'autorité compétente, comment et qui peut prendre une décision dont elle aura juridiquement à répondre ?).

Sécurité et standardisation (méthode)

Ce chapitre explique quelques nuances essentielles à la compréhension du monde de la normalisation et des évolutions actuelles dans le secteur de l'informatique de santé.

Standardisation et Normalisation

La nuance[11] entre l'activité de standardisation et celle de normalisation, et donc entre les standards (de facto) et les normes (de jure), est essentielle pour bien comprendre les évolutions actuelles et futures, en matière de modernisation de l'informatique de santé, en France notamment.

La standardisation correspond à une pratique, largement développée dans les années 80, encore très répandue dans les années 90 et, malheureusement, encore présente dans certains lieux à l'heure actuelle ; elle consiste à développer des « normes propriétaires » soit au sein de sa propre activité informatique, soit en amont chez les constructeurs et fournisseurs de matériels et logiciels informatiques. Les standards peuvent ensuite s'imposer comme normes ou normes sectorielles d'autant qu'ils répondent en général exactement au besoin, mais souvent à court terme et avec peu d'espérances d'évolutivité, d'interopérabilité voire de communicabilité d'un système à l'autre.

La normalisation, et en particulier, la normalisation en informatique de santé, s'appuie sur les normes existantes, lorsque cela est acceptable et pertinent, et à travailler ensuite à un consensus pour établir des référentiels et des documents normatifs qui conviennent à l'ensemble de la population concernée. Les normes répondent alors à l'ensemble des besoins de cette population mais elles peuvent courir le risque de n'être suffisamment pertinentes que pour une mineure partie de celle-ci ou pour un périmètre réduit de l'objectif initial. Ceci résulte souvent du lissage entre les exigences de différents acteurs majeurs très influents pour les normes nationales, ou entre les exigences de plusieurs pays normalisateurs ayant des besoins différents, pour les normes internationales.

---

10 MP6 (MPSSICSS : Modèles et Politiques de Sécurité des Systèmes d'Information et de Communication en Santé et Social) est un projet RNRT de R&D partiellement financé par la Direction de la Technologie au Ministère de la Recherche. Son objectif de proposer des modèles formels, notamment pour l'autorisation, l'anonymisation et la non-inférence.

*11 Une fois n'est pas coutume : nous avons, nous autres francophones, deux termes différents (« standard » et « norme ») pour exprimer des notions distinctes (*de facto *et* de jure*), là où les anglophones n'en n'ont qu'un (« standard »).*

Normalisation en Informatique de Santé

La normalisation en informatique de santé, qui a pris toute son importance au milieu des années 90, est relativement récente par rapport à d'autres domaines de la normalisation de l'informatique.

Ce retard s'explique car l'informatique de santé a dû se tailler une place au sein de toutes les instances de normalisation et entre les différents domaines de la normalisation en informatique. Longtemps appelée « informatique médicale » (ou « medical informatics »), elle a été rebaptisée « informatique de santé » (ou « health informatics ») en 1996 au CEN puis à l'ISO, et ensuite « informations de santé » (ou « health information systems ») en 1998 à l'AFNOR, traduisant ainsi la volonté d'être à la fois :

- assez spécialisée vers toute la sphère santé (en l'occurrence) par opposition à la normalisation dans le domaine des technologies de l'information très généraliste ;
- peu spécialisée au seul domaine médical (en l'occurrence) vis-à-vis des nouvelles tendances qui se font jour : informatique médicale, bio-informatique, neuro-informatique et autres disciplines.

Il en va de même pour la sécurité des systèmes d'information de santé au confluent de l'informatique traditionnelle, de l'informatique médicale et de l'informatique de santé et, surtout, héritant, pour le meilleur et pour le pire, d'années d'investissements en sécurité, en sécurité informatique et en sécurité des systèmes d'information (cf. notre chapitre « Histoires de sécurité »).

L'activité de normalisation en sécurité des systèmes d'information de santé doit désormais répondre à un challenge intéressant mais audacieux :

- prendre en compte l'héritage de la généricité des approches, méthodes, techniques et solutions de sécurité développées pour la sécurité des systèmes d'information en général ; cependant elle ne doit pas en abuser sous peine de n'apporter aucune valeur ajoutée aux acteurs de la santé ;
- développer autour de cet héritage tout le corpus nécessaire des notions et concepts, des méthodes et approches, des solutions et orientations, qui sont spécifiques aux besoins et aux attentes des acteurs de la santé en matière de sécurité pour la santé.

Animateur du GE-SSIS d'AFNOR et « convenor » du WG III au TC251 du CEN, je m'attache à défendre ce point essentiel tant au plan français qu'au plan européen : ne pas prendre pour argent comptant - comme cela a trop souvent été le cas - des approches ou solutions standard, inadaptées aux spécificités du secteur concerné, surtout lorsqu'il s'agit d'un secteur à haut risque ou très sensible comme celui de la santé.

Où seraient la valeur ajoutée, l'utilité et l'intérêt de groupes de travail et de normalisation qui se contenteraient de reprendre, sous leur enseigne, des normes génériques, ou a-sectorielles, déjà applicables de fait.

Si spécificités il y a, le groupe ad hoc du secteur se doit de les exprimer et de les traiter.

Évolution des normes en Informatique de Santé

Les normes développées en informatique de santé ont inévitablement suivi ce chemin (du « médical pur » à la « santé en général »). Elles sont souvent perturbées par l'apparition régulière et en progression croissante (le périmètre s'élargissant) de centres de pressions ou d'oppositions, de-ci, de-là, très souvent issus d'outre-Manche et d'outre-Atlantique. Ces perturbations compliquent fortement le processus d'obtention d'un consensus autour d'un document, norme, programme de travail, champ d'investigation ou spectre d'application.

Concernant les normes en sécurité des systèmes d'information de santé, la distinction explicitée supra entre les normes plus anciennes (cf. [8], [9], [10] et [11]), raffinant en partie des normes de sécurité génériques existantes (cf. [1], [2], [3], [4], [5], [6] et [7]) et les normes plus récentes (cf. [12], [13], [14], [15] et [16]), dédiées à la santé car nouvelles et spécifiques, traduit exactement l'évolution actuelle des normes en sécurité pour la santé.

A titre d'exemple, la norme ENV12924 [12] sur la catégorisation des protections pour les systèmes d'information de santé, actuellement en cours de révision au sein du WG III du TC251 du CEN, subit ces deux influences ; ainsi, sont à la fois exprimées :

- la volonté de prendre encore plus en compte la norme générique ISO17799 [5], qui a une finalité comparable à l'ENV12924 [12] mais avec une approche différente ;

- la nécessité de spécialiser la nouvelle version de l'ENV12924 [12] vers les besoins métier et les attentes sectorielles du monde santé et du domaine hospitalier, avec, par exemple, l'auditabilité comme nouveau critère intégré à la catégorisation.

Vers une meilleure prise en compte des normes (résultat)

Ce chapitre aborde, en amont et en aval, le problème de la trop faible prise en compte des normes en général, en santé en particulier et en sécurité notamment.

En amont, le problème réside dans le faible participation des acteurs de la santé à la construction, validation et expérimentation des normes ; même si beaucoup de raisons, tantôt légitimes (disponibilité, compétences …) tantôt non acceptables (coûts, intérêt …) pourraient être rappelées, ce que nous ne ferons pas ici, car ce n'est ni le lieu, ni l'objectif.

En aval, le problème repose sur la très faible connaissance et la trop faible prise en compte des normes de santé, et des normes en sécurité, pour pouvoir prétendre être à jour et en règle avec le minimum vital imposé, étant donné que certaines d'entre elles s'imposent de fait, même si beaucoup de raisons, tantôt légitimes (complexité du monde des normes), tantôt non acceptables (sensibilisation à l'application des normes) pourraient être rappelées, là encore.

Normes de jure plutôt que standards de facto

Il est désormais évident et admis par l'ensemble des acteurs moteurs de la modernisation des systèmes d'information de la sphère santé, qu'il est préférable de faire appel à des normes (normes de jure), si elles existent, plutôt qu'à des standards (standards de facto).

Les normes ont l'avantage d'être une base méthodologique et technologique et un référentiel commun à tout le secteur, partageable entre tous, évolutif de par l'infrastructure des instances de normalisation, interopérable par essence et communicant avec la prise en compte, actuelle des nouvelles technologies de l'information et de la communication.

Les standards, apparus avant toute exigence d'universalité, étaient des bases de travail et référentiels techniques compréhensibles à l'époque des ordinateurs centraux, où les grands acteurs pouvaient se permettre d'imposer leur loi.

Désormais, avec l'émergence des technologies intranet, extranet et internet, avec le succès du développement des réseaux ville-hôpital, avec la réalité de l'informatisation de tout le système d'information de santé, avec la volonté de modernisation des systèmes d'information hospitaliers, avec la réaffirmation de la nécessité de participation active du patient à la connaissance et à la maîtrise de son propre dossier de santé, avec l'acceptation consensuelle du dossier de santé communicant plutôt que centralisé et du dossier médical partagé plutôt que distribué, la normalisation (très active sur ces sujets) et les normes (indispensables dans ces domaines) deviennent des outils plus consensuels et pertinents que l'ancienne standardisation avec ses standards (propriétaire ou constructeur), très vite obsolètes et générateurs de surcoûts à la moindre modification significative du contexte d'application ou la moindre évolution importante de l'environnement de mise en œuvre.

Implication dans la normalisation et prise en compte des besoins sectoriels

Mais pour cela il faudra une meilleure implication de l'ensemble des acteurs de la santé dans les instances de normalisation, tant nationales et européennes, qu'internationales. Tous, sans exception, doivent pouvoir y contribuer.

L'époque de l'expression des besoins de l'utilisateur final par l'informaticien semble révolue. Par analogie, il n'est pas acceptable que les experts en sécurité des systèmes d'information - certes de santé – influencent constamment l'émergence de normes au service du patient-citoyen en particulier quant au respect de l'anonymat. Il appartient aux plus hauts responsables des institutions de la santé et des établissements de soins de porter le discours des assurés sociaux et des patients car ils représentent leurs intérêts sanitaires, individuels et collectifs, et ils sont porteurs de leurs besoins d'informations et de respect de leur intimité.

Tendances essentielles (discussion)

Des tendances essentielles se font jour qui concernent exclusivement le domaine que nous maîtrisons : la sécurité des systèmes d'information de santé (SSIS), en général, et, en particulier, la sécurité des systèmes d'information hospitaliers (SSIH).

Les cinq paragraphes suivants détaillent ces tendances émergentes, déjà abordées par les différents groupes de normalisation en santé : sécurité et qualité, sécurité et innocuité, sécurité et intimité, anonymisation et pseudonymisation et auditabilité.

Sécurité et/ou Qualité

La querelle entre la sécurité et la qualité est révolue. La sécurité, si elle est efficiente, est un apport incontestable à la qualité d'ensemble du système d'information. Inversement, la qualité des données fournies, la qualité des processus mis en œuvre et la qualité des informations générées (dont celles utiles à la gestion de la sécurité) contribuent à une meilleure sécurité du système dans son ensemble.

Le débat se situe plutôt au plan des indicateurs des niveaux de sécurité et de qualité. Une solution actuellement développée consiste à s'intéresser à la « qualité de la confiance » : quels indicateurs de confiance retenir et quelle fiabilité[12] attribuer à ces indicateurs ?

Un groupe de travail ad hoc, créé à l'AFNOR au sein de la commission de normalisation « Sécurité des Systèmes d'Information » se penche sur cette question.

En informatique de santé, un indicateur de la confiance d'un système est son niveau de sécurité et aussi, de façon récursive, la perception que chacun a de celle-ci. La communauté de l'informatique de santé fait ainsi appel à l'auditabilité du système d'information et donc, récursivement, à l'auditabilité de la sécurité même du système (cf. [12], [14], [15] et [16] et paragraphe consacré à l'auditabilité).

Sécurité-'Safety' versus Sécurité-'Security'

Dans un établissement de soins dont le métier premier est de soigner et de sauver des vies, donc la sécurité au sens d'innocuité (en français) ou au sens de 'safety' (en anglais), il est évident que toutes les priorités majeures et les décisions importantes doivent être en faveur de la sécurité-innocuité (ou sécurité-'safety').

Le problème est que cette sécurité-'safety' dépend fortement de quelques autres aspects de la sûreté de fonctionnement, dont la sécurité-'security' : en effet, une atteinte en disponibilité ou en intégrité, voire en confidentialité, sur tout ou partie du système peut avoir une incidence néfaste du point de vue de l'innocuité (i.e., on peut aisément imaginer qu'une intrusion avec intention de nuire dans un dossier de santé peut coûter la vie au patient concerné).

Des travaux ont été menés au sein du WG III du TC251 au CEN (cf. [11]), ne serait-ce que pour montrer que de nombreuses normes existent, parfois a-sectorielles, qui tentent de combiner les deux sécurités (la sécurité-'security' et la sécurité-'safety') dès lors que la qualité du système repose sur des logiciels plus ou moins critiques.

Mais là encore, l'auditabilité est un argument efficace pour traiter le fait qu'un défaut de sécurité-'security' du système puisse avoir une incidence néfaste en terme de sécurité-'safety' pour le patient, même s'il s'agit parfois plus de tirer les enseignements a posteriori pour améliorer le niveau de sécurité du système pour l'avenir.

Confidentialité-discrétion versus Confidentialité-séclusion

Au sein du quadruplet DICA – Disponibilité-Intégrité-Confidentialité-Auditabilité – qui constitue les fondements de la sécurité des systèmes d'information de santé, il est possible de distinguer deux formes de confidentialité qui ne l'étaient pas il y a encore peu de temps.

---

12 *Mais ne compliquons pas en parlant de* « fiabilité de la confiance »*, car la confiance a pour origine étymologique la notion de fiabilité et, surtout, parce qu'une fiabilité évaluée ou mesurée, une sécurité obtenue, une confiance accordée ou une qualité constatée, s'apparentent à des perceptions différentes de la même notion de sûreté de fonctionnement.*

La confidentialité classique (ici : confidentialité-discrétion) est obtenue en protégeant par des techniques réversibles (bien souvent cryptographiques) dites de chiffrement (sinon par des méthodes à base de fragmentation). Ensuite, il reste à déprotéger par des techniques cryptographiques de déchiffrement cette fois (sinon par dé-fragmentation) les informations nécessitant une certaine discrétion : ainsi, par exemple, un extrait de dossier médical échangé par messagerie sur un réseau entre deux professionnels de santé.

Avec ce type d'exigence en confidentialité-discrétion, il est toujours possible de lever la discrétion (cf. déchiffrement après chiffrement, dé-fragmentation après fragmentation) :

- soit légitimement, par cryptographie, pour l'utilisateur habilité ayant reçu autorisation d'accéder et d'utiliser la bonne clé de dé-protection (clé de déchiffrement ou de dé-fragmentation) ;
- soit illégitimement, par cryptanalyse, pour le « hacker » non habilité forçant la technique de protection utilisée (cryptographique ou autre), lorsque celle-ci n'est pas suffisamment robuste ;

La confidentialité d'un nouveau type (ici : confidentialité-séclusion) est obtenue en protégeant de façon irréversible et robuste à toute tentative d'indiscrétion, l'information sensible nécessitant plus qu'une certaine discrétion et soumise à une volonté délibérée de séclusion[13]. On parle d'anonymat, d'intimité, de vie privée ou, plus généralement et dans le cadre de cet article : d'intimité électronique.

Si la technique mise en œuvre pour répondre à une exigence de confidentialité-séclusion est suffisamment robuste, tant mathématiquement, que statistiquement, ou par la logique ou par cryptanalyse, alors il sera possible de « lever » la séclusion (expression antinomique), contrairement à la discrétion. C'est donc le concept idéal pour prendre en compte le respect de la vie privée, la notion de « colloque singulier » reclus entre un patient et son médecin et aussi pour garantir la non-divulgation d'informations individuelles et à caractère médical, de soin, de santé, qu'elles soient nominatives ou même anonymes.

En sécurité des systèmes d'information de santé, tant au plan français par le document normatif auquel nous avons fortement contribué (cf. [15]) qu'au plan européen auquel un sujet de travail a été accepté depuis 2000, ces travaux de distinction entre la discrétion et la séclusion ont été perçus comme précurseurs vis-à-vis de l'identification du patient et aussi novateurs pour des secteurs autres que la santé (cf. paragraphe sur l'anonymisation).

Mais, à nouveau, s'il n'y a pas de confiance, ni d'auditabilité, sur l'efficience d'une réelle séclusion par rapport à de la discrétion classique, cela ne sera que de peu d'intérêt.

Anonymisation ou Pseudonymisation

L'anonymisation consiste à remplacer les données d'identification d'un individu et toutes les informations identifiantes le concernant par des numéros ou « identifiants » qui doivent être à la fois muets (c'est-à-dire sans sémantique) et anonymes (c'est-à-dire sans retour possible vers l'identité de l'individu) ; en contre-exemple, citons le numéro INSEE (dit « numéro de sécu. ») qui renseigne sur le sexe, la date et le lieu de naissance et est en bijection avec, actuellement, le nom de l'assuré social (Vitale1) et, à l'avenir, avec celui du patient (Vitale2).

La pseudonymisation consiste à remplacer toujours et partout (pour un contexte et un périmètre donnés, comme par exemple les statistiques du PMSI) l'identifiant d'un même individu par le même numéro ou « identifiant » anonyme dit pseudonyme : il s'agit donc d'une anonymisation toujours et partout la même, dont avec pseudonyme.

Il faut surtout avertir qu'une donnée anonymisée (ou, surtout[14], pseudonymisée) n'est pas irrémédiablement anonyme : car elle reste une donnée individuelle donc à caractère personnel, et elle le restera tant qu'elle ne sera pas agrégée. Il peut paraître paradoxal de proclamer qu'« anonymisé » ne veut pas forcément dire « anonyme ». Comme le montrent toutes les techniques d'inférence

---

13 La « séclusion » est une forme de réclusion décidée de son plein gré par l'individu concerné, lorsque celui-ci souhaite préserver son intimité vis-à-vis des agressions externes.

14 Anonymisée ou, surtout, pseudonymisée : *une information anonymisée (un épisode de soin des statistiques PMSI), lorsqu'elle est chaînée par le même pseudonyme anonyme avec d'autres informations anonymisées (trajectoire de soins des statistiques PMSI), devient une information corrélée (i.e, pseudonymisée) bien plus vulnérable vis-à-vis des risques de désanonymisation que lorsqu'elle était isolée (i.e., anonymisée sans être pseudonymisée).*

(déductive, inductive, abductive et « adductive ») issues de la logique du premier ordre et aussi de la logique modale, il est possible de recouvrer des informations nominatives à partir de données pourtant anonymisées.

On voit là tout l'intérêt mais aussi les limites des différents avis prononcés par la CNIL – Commission Nationale de l'Informatique et des Libertés – permettant de dire que des données sont ou non nominatives, bien que demeurant toujours à caractère personnel.

Divers travaux effectués ou en cours, mentionnés précédemment (cf. [15] à l'AFNOR et sujet de travail au WG III du TC251), abordent ce sujet pour lequel il n'y a pas encore de fondement scientifique établi, alors qu'il s'agit d'un problème de société. Imaginez l'émoi si, lors de la publication par un établissement de soins, sur son site web, de ses statistiques concernant les pathologies traitées et les populations de patients soignés, un « hacker » mal intentionné, ou animé de visées mercantiles, pouvait ré-identifier la majeure partie des patients constituant toutes ces statistiques, en utilisant les différentes techniques d'inférence évoquées supra… !

Auditabilité plutôt que 'Accountability'

L'auditabilité (littéralement : « capacité à être audité ») ne doit pas être confondue avec la propriété de « accountability » (dont une mauvaise traduction de l'anglais est : traçabilité).

Cette « accountability » (traduction littérale : « capacité à rendre compte ») est à rapprocher de la technique de non-répudiation issue originellement de la norme ISO 7498-2 qui s'adressait aux échanges et protocoles des couches OSI. Elle se situe surtout à un niveau technique :

- non-répudiation par l'origine d'un message de l'émission de ce message ;
- non-répudiation par la destination d'un message de la réception de ce message ;
- non-répudiation par l'origine du message de sa remise à un opérateur télécom ;
- non-répudiation par la destination du message de sa livraison par l'opérateur télécom.

L'auditabilité se situe plus à un niveau juridico-technique englobant les diverses notions techniques de traçabilité (trace d'une action), imputabilité (imputation de cette action à un rôle), et aussi les notions juridiques d'opposabilité (opposer devant un juge un élément probant), voire irréfutabilité (lors d'un jugement sur la base d'éléments probants). Avec l'apparition en Europe (directive européenne) et en France (loi, décrets et arrêtés), de la force probante de la « signature électronique » (anciennement dite « signature numérique »), ces notions juridico-techniques prennent tout leur sens dans le contexte sensible de la santé.

Évoquée à plusieurs reprises, à travers les diverses perceptions traitées dans cet article, l'auditabilité constitue l'apport majeur de l'activité en sécurité des systèmes d'information de santé. Rendre un système d'information (hospitalier, par exemple) capable d'être audité pour permettre d'en évaluer sa qualité et, similairement, rendre aussi la sécurité de ce système d'information (hospitalier, dans notre exemple) capable d'être auditée pour permettre d'en estimer sa confiance ou la qualité de cette confiance, est un plus. C'est le minimum que doit apporter la normalisation en sécurité des systèmes d'information de santé (cf. [14], [15], et [16]), à laquelle nous avons contribué depuis quelques années.

Si l'« accountability », notion pourtant sémantiquement forte (capacité à rendre compte), est devenue une propriété assez faible (restreinte à des techniques de non-répudiation), alors l'auditabilité, notion à la fois technique (reprenant en cela l'« accountability ») et juridique (innovant en cela autour de la « signature électronique »), est indispensable au développement futur des systèmes d'information de santé, des systèmes hospitaliers en premier lieu.

Quel avenir pour les normes en sécurité/santé (conclusion)

De nombreux travaux normatifs ont déjà été effectués en informatique de santé et en sécurité des systèmes d'information de santé, mais il reste beaucoup à faire :

- de nouveaux chantiers sont en cours avec l'émergence de l'ISO17799, les révisions de l'ENV12924 et de l'ENV13606-3 et la probable révision de l'ENV13608-1 ;
- l'appellation « systèmes d'information et de communication » prend tout son sens dans le secteur hospitalier avec les considérations de sécurité à associer au respect de l'intimité du

patient et au colloque singulier, au dossier de santé communiquant (pas obligatoirement communiqué), au dossier médical partageable (pas systématiquement partagé), à la confiance accordée en générale aux SICH et à leurs sécurité associées.

De nombreux concepts et aspects fondamentaux, sur lesquels nous travaillons depuis de nombreuses années, ont pris leur place dans des normes nationales, européennes ou internationales et commencent à être utilisés de façon opérationnelle dans les établissements : respect de l'anonymat, anonymisation et pseudonymisation, politique de partage des informations, nécessité d'auditabilité pour les SICH et ainsi volonté de partager, avec les utilisateurs finals, la confiance placée dans de tels systèmes.

Mais encore faudra-t-il, pour que ces efforts plus ou moins aboutis perdurent, que tous les acteurs de la santé et du monde hospitalier prennent conscience de la nécessité de :

- s'appuyer sur la normalisation en santé qui est à la fois flexible et pertinente ;
- contribuer à la normalisation en sécurité pour qu'elle soit encore plus efficiente ;
- s'opposer à la normalisation parfois imposée d'Outre-Manche ou d'outre-Atlantique, selon des visions souvent trop éloignées de l'éthique et de la déontologie françaises et européennes.

Remerciements

Mes remerciements à l'ensemble des participants, experts-sécurité, professionnels de santé, ingénieurs en normalisation, fidèles et assidus [ils se reconnaîtront] aux groupes sécurité (AFNOR/CNIS/GE-SSIS et CEN/TC251/WG III) que j'ai l'honneur et le plaisir d'animer avec toute ma sincérité.

Remerciements également aux organisateurs de ce colloque qui m'ont donc permis de (faire l'effort pour trouver le temps pour) rédiger ces quelques propos, ainsi qu'aux re-lecteurs du comité scientifique qui m'ont apporté leurs précieux retours sur cet article.

Toute ma reconnaissance enfin, au comité de lecture de la Lettre ADELI, et surtout à Alain Coulon qui, comme à son habitude, a pris le plus grand soin à relire et corriger cette version de mon article pour une parution en avant première dans cette Lettre ADELI.

Dr Gilles TROUESSIN
Ernst & Young – Audit et Sécurité des Systèmes d'Information
1, place Alfonse Jourdain – 31000, TOULOUSE
Tél. : 05 62 15 51 36 – Fax : 01 58 47 10 33
gilles_trouessin@ernst-young.fr

Biographie

Gilles TROUESSIN est Docteur en Sécurité et Sûreté de Fonctionnement depuis 1991. Il s'est spécialisé dans la Sécurité des Systèmes d'Information de Santé depuis 1993 et il a été ensuite nommé expert-normalisation en Informatique de Santé en 1996, 1997 et 1998, respectivement à l'AFNOR, au CEN et à l'ISO.

Depuis 1996, il a participé à la création, il contribue activement et, surtout, anime le Groupe d'Experts en Sécurité des Systèmes d'Information de Santé (GE-SSIS) d'AFNOR.

Depuis 1997, il participe activement au Working Group on Security Safety and Quality du Technical Commitee 215 – Health Informatics au CEN – Comité Européen de Normalisation, dont il a été élu Convenor en septembre 2001.

Il participe régulièrement aux travaux du Working Group on Security et du Working Group on Health Card du Technical Commitee 215 – Health Informatics de l'ISO – Organisation Internationale de Standardisation'.

Bibliographie

[1] ISO 7498-2:1989 Information processing systems -- Open Systems Interconnection -- Basic Reference Model -- Part 2: Security Architecture.

[2] TCSEC -- Trusted Computer Security Evaluation Criteria, 1985.

[3] ITSEC -- Information Technology Security Evaluation Criteria, 1991.

[4] ISO 15408-1 ISO/IEC Information Technology -- Security Techniques Evaluation for IT security -- Part 1: Introduction and general model

[5] ISO 17799 -- Code of Practice for Information Security Management

[6] GMITS 1-5:

ISO 13335-1 ISO/IEC Information Technology – Guidelines for management of IT Security-Part 1: Concepts and Models for IT Security

ISO 13335-2 ISO/IEC Information Technology – Guidelines for management of IT Security-Part 2: Managing and planning IT Security

ISO 13335-3 ISO/IEC Information Technology – Guidelines for management of IT Security-Part 3: Techniques for management of IT Security

[7] ISO 10181 1-7 :

ISO/IEC 10181-1:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Overview

ISO/IEC 10181-2:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Authentication framework

ISO/IEC 10181-3:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Access control framework

ISO/IEC 10181-4:1997 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Non-repudiation framework

ISO/IEC 10181-5:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Confidentiality framework

ISO/IEC 10181-6:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Integrity framework

ISO/IEC 10181-7:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Security audit and alarms framework

[8] ENV12251 Health Informatics -- Secure User Identification for Healthcare -- Identification and Authentication by Passwords - Management and Security

[9] ENV13729 Health Informatics -- Secure User Identification -- Strong Authentication using Microprocessor Cards

[10] ISO WD 17090 Public Key Infrastructure

[11] CR13694:1999 Health Informatics – Safety and Security related Software Quality Standards for Healthcare

[12] ENV12924 :1996 Security Categorisation and Protection for Healthcare Information Systems

[13] ENV13606-3 Health Informatics -- Electronic Healthcare Record Communication – Part 3: Distribution Rules

[14] ENV13608-1:1999 Health Informatics -- Security for Healthcare Communication – Part 1: Concepts and Terminology

[15] FD S 97-560 -- Fascicule de Documentation -- Informatique de Santé -- Anonymisation -- Glossaire, démarche d'analyse et expression de besoins

[16] FD S 97-700 -- Fascicule de Documentation -- Informatique de Santé -- Glossaire – Sécurité des Systèmes d'Information de Santé