ORDRE DES MEDECINS
CONSEIL NATIONAL

ORDE DER ARTSEN
NATIONALE RAAD

Sécurité des données transmises par Internet

Doc	a084020
Date de publication	20/02/1999
Origine	NR
Thèmes	Informatique Secret professionnel

Un Conseil provincial fait parvenir au Conseil national plusieurs questions émanant du "Medisch Discussieforum", asbl, concernant les données médicales et la télématique :

1. Les médecins peuvent-ils -bien entendu en respectant les règles de la déontologie médicale et les garanties en matière de secret professionnel- échanger des données via l'Internet et/ou consulter des informations relatives aux données médicales des patients qu'ils traitent?
2. Il existe à l'heure actuelle des programmes (entre autres PGP) jouissant d'une reconnaissance et d'une considération internationale et offrant toutes les garanties au niveau de l'encryptage des données échangées. Ces programmes peuvent-ils être utilisés pour la conservation et l'échange de données médicales comme décrit sous la question 1?
3. Ces programmes d'encryptage fonctionnent au moyen d'une double clé, une clé privée (secrète) et une clé publique de préférence la plus répandue possible. La certification de l'authenticité de cette clé publique par une partie fiable est une bonne habitude et une garantie supplémentaire. L'Ordre des médecins est-il disposé à assumer cette fonction, soit entièrement (en certifiant lui-même), soit en partie (en confiant ce travail à une autre partie fiable, par lui agréée)?

Le Conseil provincial pose, en outre, la question de savoir si des données médicales confidentielles peuvent être échangées via Internet.

Réponse du Conseil national :

Lors de sa séance du 20 février 1999, le Conseil national a examiné votre lettre du 6 janvier 1999 relative à l'échange de données médicales confidentielles via Internet ainsi que de la documentation y annexée.

Le Conseil a l'avantage de vous transmettre ci-joint une note relative au problème de la sécurité de données transmises par Internet.
En ce qui concerne les questions précises posées par le Medisch Discussieforum, les réponses suivantes ont été formulées :

1. L'échange de données via l'Internet doit se faire conformément aux instructions données par les avis du 16 avril 1994 et du 22 avril 1995.
2. Les programmes utilisant un chiffrement asymétrique pour l'échange des données et ceux utilisant un chiffrement symétrique pour la conservation des données assurent une protection valable conditionnée par le type d'algorithme et la longueur des clés dont il est fait usage ainsi que par le respect des mesures de sécurité recommandées. Dans les conditions présentes, les clés RSA de 1024 bits

au moins offrent satisfaction en ce qui concerne la sécurité.
3. Ainsi qu'il a déjà été signalé précédemment (avis du 22 avril 1995 -1.6-), l'Ordre des médecins peut assumer la fonction de certification des clés publiques.

Note concernant la sécurité des données transmises par Internet :

Il est notoire que des données circulant sur Internet peuvent être lues par des personnes non concernées par l'échange de ces données. De même, il est connu depuis bien longtemps que ces mêmes personnes peuvent accéder aux contenus des disques d'ordinateur lorsque ceux-ci sont connectés au réseau téléphonique.
La protection de l'accès au moyen de mots de passe est devenue illusoire. Les briseurs de code (Hackers) se font un jeu de deviner et de contourner, en recourant parfois à des moyens techniques extrêmement puissants, les barrières mises en place par les individus, les sociétés et les institutions pour se protéger. Le Chaos Computer Club a engendré des émules travaillant pour le grand banditisme, les mafias et les Etats ! Des règlements de comptes ne sont pas exceptionnels, certains individus ont acquis une réputation considérable grâce à leurs prouesses de décodage, certains ont été emprisonnés, d'autres sont morts dans des conditions suspectes (1), beaucoup courent encore.

Les exploits des hackers ne servent pas uniquement leur passion de briseurs de code désintéressés.

L'espionnage industriel est pratiqué sur une grande échelle et par des moyens proportionnels à la puissance des sociétés en concurrence. Des exemples récents, notamment dans l'industrie automobile, illustrent ce fait. Mais la pratique semble fréquente. Parfois même la simple surveillance des destinataires de courrier électronique peut suffire pour connaître des informations commercialement ou techniquement utiles.

Grâce à la puissance de travail des outils informatiques la constitution de fichiers et l'exploitation des bases de données est devenue aisée et à la portée de chacun.
On a vu se multiplier ces bases de données dans le secteur de la santé. Une Banque Carrefour des données de la sécurité sociale a vu le jour dans notre pays.
Une législation européenne a été créée pour protéger la vie privée (2). La Belgique vient de transposer cette directive dans la loi du 8 décembre 1992 (3).
S'il existe un cadre légal de protection des données à caractère personnel, celles-ci restent cependant l'objet de convoitises et d'agressions fréquentes et aisées.
En effet, la généralisation de l'informatique et des échanges par voie électronique permet d'accéder à des données privées non seulement au sein des ordinateurs où elles sont stockées mais même pendant qu'elles circulent sur les réseaux !
Leur protection est donc devenue cruciale.

Depuis la nuit des temps, les États tentent de s'emparer des secrets de leurs voisins. Cela constitue le plus clair des activités des services secrets. Depuis très longtemps les systèmes de protection font appel au codage des données pour les rendre indéchiffrables. Ceci est l'origine des services du chiffre dans les Ambassades.
Celui qui détient un code non violable est gagnant. On connaît l'aventure de la machine Enigma mise au point pendant la dernière guerre. Et une fois de plus c'est l'informatique, avec sa puissance et sa vitesse de calcul, qui a permis aux mathématiciens de créer des algorithmes de chiffrement de plus en plus complexes et longs, choisis de manière aléatoire, qui offrent une protection réputée totale.
Comme il se doit, des ordinateurs de plus en plus puissants sont alors mis en batterie pour tenter de casser le chiffre. L'escalade n'est pas proche de s'arrêter.
Des sociétés de sécurité organisent même des compétitions entre casseurs de code pour tester et mettre à l'épreuve des algorithmes connus et montrer leur éventuelle

fragilité (4).
La presse publie également les exploits de jeunes génies en mathématiques qui élaborent des algorithmes dits incassables mais dont le devenir ultérieur ne nous est pas connu (5).

En fait, il importe que les utilisateurs d'Internet soient adéquatement informés de ce qu'ils font et des risques encourus en fonction du type de communication qu'ils réalisent.
En effet les dangers diffèrent s'il s'agit de laisser une base de données accessible sur un site, de donner des ordres d'achat ou bancaires ou de communiquer des données via un serveur de courrier à une personne identifiée.

Affirmer que le réseau Internet est aussi perméable qu'un panier est parfaitement exact. C'est d'ailleurs son accessibilité qui constitue son attrait principal. La règle de ne jamais confier de numéros de cartes bancaires ou autres est rappelée automatiquement sur l'écran chaque fois qu'une transaction est initiée. De même que l'on ne confie pas à la poste des lettres personnelles sous enveloppe ouverte ou sur carte postale, on ne peut évidemment confier aucun écrit de quelque importance privée au réseau Internet. Car dans ce dernier cas ce n'est pas seulement le facteur qui risque de connaître vos secrets mais le monde entier.
Toute donnée privée qui circule sur ce réseau doit être rendue illisible pour ceux qui ne sont pas concernés.

Les Organisations Européennes soutiennent explicitement la nécessité du recours au contrôle des accès, à la cryptographie, à la certification des clés et à la signature digitale (6). La standardisation des procédures est en voie de réalisation (7). En Belgique la loi du 19 décembre 1997 permet sans restriction le recours à la cryptographie (8).

Le Conseil National n'a pas autorisé, jusqu'à présent, que des bases de données médicales relatives à des individus directement ou même indirectement identifiables, résident en permanence sur un site Internet.
C'est dans cette optique qu'ont été découragées des initiatives de mise à disposition de dossiers médicaux, même protégés par des codes d'accès contrôlés par les patients concernés, les médecins de garde, etc.

Seules ont fait l'objet de réglementations les échanges de données médicales entre médecins par l'intermédiaire d'un serveur jouant le rôle de boite aux lettres (9, 10, 11, 12).
Le Conseil a chargé les conseils provinciaux de vérifier les contrats entre médecins et fournisseurs de service et le respect des instructions de sécurité données.

En ce qui concerne ces conventions rappelons quelques conditions de fonctionnement qui doivent être spécifiées :

- le serveur ne peut être utilisé pour d'autres applications que le transfert de données médicales.
- il ne peut contenir que des données chiffrées (encryptées) et il ne peut avoir accès aux clés.
- les données contenues dans le serveur doivent être automatiquement effacées après qu'elles ont été déchargées par le destinataire et de toute manière après un délai court – 10 ou 15 jours maximum – lorsque celui-ci n'a pas consulté sa boîte aux lettres.
- le système doit être ouvert, c.a.d. accessible à tous les utilisateurs médecins, ce qui implique l'emploi d'un format standard lisible par les programmes usuels.
- le gestionnaire du système est responsable du contrôle des procédures de sécurité.

Les médecins qui utilisent le système d'échange de données ont l'obligation de veiller au respect du secret professionnel et sont responsables des mesures de sécurité. Ceci suppose notamment que :

- les clés de chiffrement soient générées exclusivement au sein de son ordinateur par le médecin.
- l'algorithme utilisé offre des garanties de solidité suffisantes au regard des données actuelles en la matière, en particulier en ce qui concerne la longueur des clés asymétriques (13) et la longueur de la partie symétrique.
- les clés publiques soient certifiées par une autorité de confiance.
- la clé secrète soit protégée par une phrase de passe, régulièrement modifiée selon les circonstances, et qu'elle soit conservée sur un support séparé lorsqu' il s'agit d'un terminal utilisé par plusieurs utilisateurs.

Le Conseil national s'est proposé pour certifier les clés publiques, ce qui implique qu'il y apposera sa signature électronique garantissant de la sorte l'authenticité de cette clé.

Le rôle des Conseils provinciaux est entr'autres de contrôler les garanties de confidentialité offertes par les contrats conclus entre médecin et fournisseur de services de messagerie électronique. Ceci implique l'appréciation de la solidité des algorithmes et du respect des conditions de sécurité prônées par l'Ordre.

Le problème de la certification des clés, qui arrivent aux Conseils provinciaux, se pose au niveau national.

La création d'une structure d'échange d'informations entre Conseils provinciaux et Conseil national s'avère indispensable afin de transmettre les clés certifiées et d'informer au sujet des contrats approuvés, des progrès de la recherche concernant les techniques, etc. Pareil outil pourrait aisément fonctionner par échange de courrier électronique et ne nécessiter que des réunions espacées.

En conclusion, la confidentialité des données échangées via Internet peut être totalement assurée par un chiffrement utilisant des méthodes fiables dont la solidité est abondamment confirmée par la littérature scientifique (14, 15).

Références :

1. http:/\www.lalettre.com/nexs/jan/201099_4.html
2. Directive 95/46/CE/ du 24 octobre 1995
3. Loi du 11 décembre 1998 transposant la directive 95/46/CE
4. DES Challenge III, RSA Laboratories, http://www.rsa.com/rsalabs/des3/ index.html
5. Magee, A. Teenager cracks e-mail code. The Times of London, 13 Jan. 1999
6. Comité Permanent des Médecins Européens : Security in Clinical Information Systems, BMA paper, 24/08/1998
7. Comité Européen de Normalisation CEN/tc 251/wg6
8. Loi du 19 decembre 1997
9. Boîte aux lettres électronique - Laboratoires. Conseil national Bulletin 63-19
10. Transmission de courrier par la " voie télématique". Conseil national Bulletin 63-21
11. Messageries électroniques. Conseil national Bulletin 65-22
12. Communications électroniques - Secret médical. Conseil national Bulletin 69-13
13. Dragan, R. Encryption. PC Magazine June 9, 1998
14. Toward An Electronic Patient Record '95 Orlando, FL. March 1995
15. Barber, B. Treacher, A. & Louwerse, C.P. Towards Security in Medical Telematics. IOS Press. Amsterdam 1996

La note figurant ci-dessus a également été transmise aux autres Conseils provinciaux.