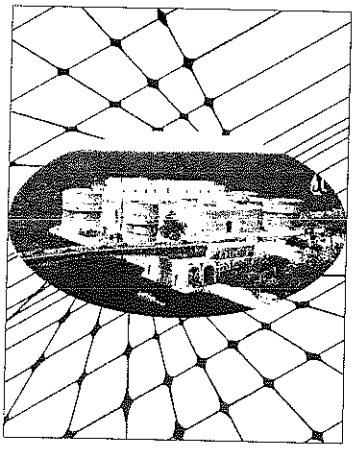
Associazione Italiana di Informatica Medica

1981 - 1998

L'Informatica Medica in Italia e in Europa: storia, evoluzione, prospettive



Atti del X Congresso Nazionale di Informatica Medica

Taranto, 15 - 17 Ottobre 1998
Space Software Italia
e
La Cittadella della Carita'

a cura di

P.L. Ballesio - A. Serio - R. Maceratini

Volume II

PROTEZIONE DEI DATI E POLITICHE DI SICUREZZA: UNA SPERIMENTAZIONE IN CAMPO RADIOLOGICO

Caramella Davide[1], *Dell'Osso Ruggero*[1], *Fabbrini Fabrizio*[2], *Fusani Mario*[2], *Perron Camus Giorgio*[1]

[1]Dipartimento di Radiologia, Università di Pisa
[2]Istituto di Elaborazione dell'Informazione, CNR,
Via S. Maria 46, 56126 Pisa

Riassunto

Protezione dei dati, riservatezza e sicurezza dell'informazione costituiscono requisiti fondamentali per il corretto utilizzo delle tecnologie dell'informazione in ambito medico.

Questa memoria propone una panoramica delle problematiche relative a sicurezza e riservatezza in generale e in ambito medico in particolare, con riferimento al crescente utilizzo di tecnologie telematiche.

Viene infine descritta la sperimentazione condotta presso il Dipartimento di Radiologia dell'Università degli Studi di Pisa, relativa alla protezione delle immagini radiologiche e della loro trasmissione sicura su rete pubblica.

Introduzione

Lo scopo di una politica di sicurezza nella gestione di un sistema informativo sanitario è quello di fornire un meccanismo affidabile per condividere l'informazione, che assicuri la continuità del servizio e minimizzi il possibile danno annullando o minimizzando l'impatto degli incidenti riguardanti la sicurezza.

La gestione della sicurezza dell'informazione ha tre componenti principali:

- *Confidenzialità*: proteggere l'informazione sensibile dalla divulgazione non autorizzata.
- *Integrità*: salvaguardare la correttezza e la completezza dei dati e dei programmi.
- *Disponibilità*: garantire che dati e servizi di calcolo siano disponibili agli utenti che li richiedano.

Lo schema generale di approccio alla sicurezza consiste dei seguenti passi:

1. Identificazione delle risorse da proteggere.
2. Identificazione dei rischi.
3. Definizione di una scala di priorità conseguente alla valutazione dei rischi.

4. Scelta ed implementazione delle contromisure, se necessarie.

Problematiche di sicurezza

In linea con questo schema, verranno discusse alcune "minacce" alla sicurezza dei dati relativi alla stato di salute dei singoli individui che possono derivare dalla automazione ed in particolare dal fatto che molti sistemi ospedalieri, su cui risiedono dati clinici, sono collegati in rete tra loro. Tali minacce ricadono solitamente in tre categorie principali, secondo il loro scopo, che può essere:

- Il furto di informazione.
- Privare gli altri dell'uso del sistema: tutti sono a conoscenza del fenomeno dei virus e dei loro effetti negativi.
- Alterare l'informazione. Queste possono essere a loro volta classificate come *naturali*, se originate da guasti fisici di origine naturale, come il processo di invecchiamento dei materiali; *colpose*, se originate da errori umani non intenzionali, come errori di programmazione che, generando errori software, portino ad una alterazione dei dati; *premeditate*, se originate da tentativi intenzionali di modificare i dati.

Tecniche per la sicurezza

Per prevenire o minimizzare i problemi relativi alla sicurezza, devono essere stabilite delle appropriate tecniche di controllo. Tali tecniche includono solitamente controlli di tipo fisico, controlli di tipo procedurale e controlli di tipo tecnico: il loro scopo comune è quello di stabilire differenti livelli di accesso al sistema informativo, responsabilizzare gli utenti, mantenere fisicamente separati utenti, programmi e dati, identificare e tracciare le operazioni illegali.

Le contromisure di tipo fisico includono l'impiego di personale di sorveglianza e l'utilizzo di aree ad accesso ristretto, insieme con strumenti come porte blindate, ecc.

Il loro scopo è la protezione diretta del sistema di calcolo, delle relative apparecchiature e dei contenuti contro i danni causati da persone non autorizzate.

I controlli di tipo procedurale - talvolta noti come politiche organizzative - coinvolgono soprattutto l'elemento umano e non sono meno rilevanti dei meccanismi fisici e tecnici nel proteggere l'informazione sanitaria e la privacy del paziente: le migliori contromisure di tipo tecnico e fisico infatti potrebbero risultare scarsamente efficaci se non correttamente implementate.

Gli strumenti tecnici per la sicurezza consistono in un insieme di pratiche e meccanismi di tipo tecnologico, riguardanti hardware, software

e sistemi di comunicazione, che vanno dai sistemi automatici per il rilevamento e il recupero dell'errore a strumenti molto più sofisticati come i sistemi di Autenticazione e Certificazione e la Crittografia.

L'autenticazione è un qualsiasi processo di verifica dell'identità dell'origine di una richiesta di informazione in un sistema di elaborazione. In genere, l'autenticazione si basa su uno o più dei criteri seguenti:

- Qualcosa che indica dove ci si trova (un indirizzo di rete, un numero di telefono in uno schema di connessione di tipo *call-back*, un terminale collegato su una linea dedicata): *authentication by location*.
- Qualcosa di cui si è a conoscenza (una password, un numero di codice): *authentication by knowledge*.
- Qualcosa relativo alla propria persona (la firma, le impronte digitali, l'impronta retinica, lo spettro vocale): *authentication by characteristics*.

Con la crittografia, il messaggio originale (messaggio *in chiaro*) viene trasformato in una forma non intelligibile (messaggio crittografato, o *crittogramma*) mediante l'uso di un algoritmo e di una regola di trasformazione (*chiave*), per salvaguardarne sia la confidenzialità che l'integrità durante la trasmissione e l'archiviazione, rendendone così inutile l'intercettazione.

Al momento due tipi di crittografia sono comunemente impiegati: a chiave segreta, un sistema in cui la stessa chiave viene utilizzata sia per codificare che per decodificare (algoritmi simmetrici) e a chiave pubblica, un sistema in cui vengono utilizzate due chiavi diverse, una per crittare e l'altra per decrittare, una sola delle quali necessita di essere mantenuta segreta (algoritmi asimmetrici).

Reti di calcolatori

Prima del diffondersi delle reti di calcolatori, l'informazione di tipo sanitario aveva una localizzazione fisica, era difficile da copiare e comunque accessibile solo in modo centralizzato. L'automazione e la connessione in rete hanno cambiato questa situazione completamente: il dato non ha più necessariamente una localizzazione fisica, può essere copiato con estrema facilità ed è accessibile da siti remoti: l'esistenza di *Internet* significa che i dati possono essere trasferiti in un computer dislocato in un punto qualsiasi nel mondo, con la stessa facilità con cui possono essere spostati sulla scrivania accanto alla nostra.

Un modo di tenere sotto controllo gli accessi esterni ad una rete locale è quello di ricorrere alla tecnologia dei *firewall*.

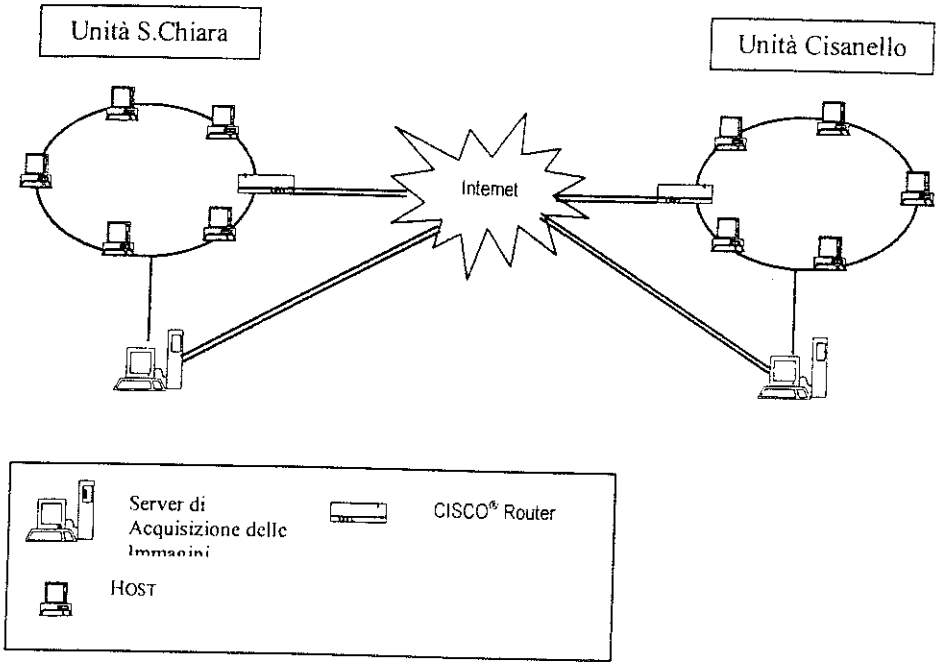
Un firewall è essenzialmente un elemento di una rete locale in cui vengono concentrati tutti gli accessi da parte di utenti esterni, controllato da un sistema che può essere configurato per "filtrare" tali accessi in modo da ottenere un alto livello di sicurezza. Questo viene generalmente ottenuto implementando un meccanismo di autenticazione e permettendo l'utilizzo solo dei servizi "sicuri" (*trusted services*). Il firewall viene usualmente interposto tra la rete interna fidata e la connessione esterna ad Internet e configurato in modo da:

- impedire che una workstation esterna possa mimetizzarsi da workstation interna fidata (*spoofing*);
- impedire lo stabilirsi di connessioni non sicure;
- impedire ad un qualsiasi utente esterno di vedere informazione della rete interna (nomi, indirizzi, ecc.);

Ovviamente, un firewall non può offrire da solo la soluzione perfetta: da un certo punto di vista, è solo un ulteriore computer o un ulteriore software da aggiungere ad un sistema già complesso. Nonostante ciò, costituisce uno strumento importante anche perché contribuisce a focalizzare l'attenzione dell'amministratore del sistema su un numero limitato di punti vulnerabili di una organizzazione generalmente complessa, ed aiuta a tenere sotto controllo almeno i tipi di attacco più usuali.

La sperimentazione condotta

Il Dipartimento di Radiologia dell'Università degli Studi di Pisa è costituito da due strutture separate, una dislocata all'interno dell'Ospedale S.Chiara, che indicheremo come Unità di S. Chiara, ed una presso l'Ospedale di Cisanello, che chiameremo Unità di Cisanello. Ciascuna di queste strutture dispone di una rete locale (LAN) connessa ad Internet. All'interno di ciascuna rete di ogni dipartimento è presente un server di acquisizione d'immagini dotato di due interfacce di rete; una verso la LAN del proprio dipartimento, l'altra verso la MAN (Metropolitan Area Network) alla quale la struttura ospedaliera si appoggia per le applicazioni di trasmissione delle immagini. Quest'ultimo collegamento è stato predisposto in modo da avere una connessione ad alta velocità totalmente dedicata allo scambio di immagini tra l'unità di S. Chiara e l'unità di Cisanello. La situazione appena descritta è schematizzata nella figura:

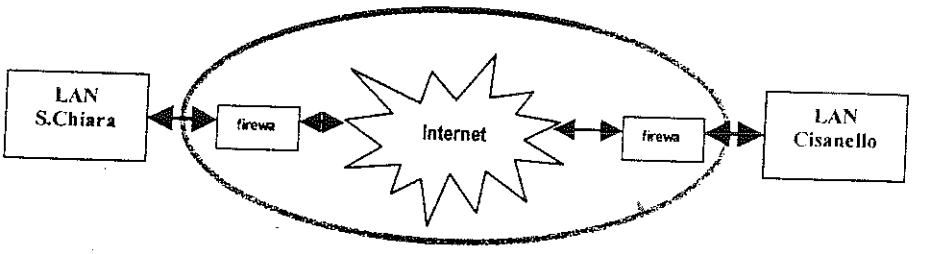


La necessità di lasciare accesso alle immagini radiologiche memorizzate nel server di acquisizione deriva dal fatto che le immagini radiologiche sono informazioni indispensabili per le attività diagnostiche e quindi devono essere prontamente disponibili all'intero Dipartimento. Inoltre rispetto ad altri tipi di dati, che potrebbero essere comunicati anche via telefono o fax, la possibilità di acquisizione delle immagini si riduce alla semplice consegna materiale delle stesse, oppure alla più comoda ed efficiente trasmissione su rete, che ha anche il vantaggio di essere più veloce. Quest'ultima soluzione è ancora più apprezzata quando lo scambio ed il consulto delle immagini deve avvenire tra unità separate, come nel caso presentato di un dipartimento costituito da due entità oppure come nel caso di strutture dislocate in città diverse; in tali casi i vantaggi della trasmissione su rete sono ancora più evidenti.

Come svantaggio abbiamo il fatto di dover effettuare una trasmissione di dati sensibili attraverso una rete pubblica che non tutela da malintenzionati o da potenziali attacchi; questo comporta tutti i problemi precedentemente introdotti relativi alla sicurezza e alla privacy dei dati trasmessi. Occorre inoltre inquadrare le eventuali soluzioni all'interno di una più generale politica di sicurezza; non solo occorre rendere la trasmissione sicura in modo da proteggere le informazioni in

transito, ma è indispensabile garantirne l'integrità e la disponibilità in loco.

È stata delineata una soluzione in due passi: il primo passo è quello di proteggere le reti locali delle due unità tramite l'installazione di un firewall specificatamente configurato tra ciascuna rete locale e Internet. È stato implementato un *proxy* che, oltre ad effettuare il filtraggio dei pacchetti, consentisse di effettuare la certificazione del client e del server.



Il secondo passo è quello di usare la crittografia per implementare una trasmissione sicura su rete pubblica, mediante la realizzazione di una *Virtual Private Network* su cui scambiare in maniera sicura dati fra le Unità di S. Chiara e di Cisanello attraverso un canale *privato*, *autenticato* e *fidato*.

Bibliografia

[1] *Data Protection and Confidentiality in Health Informatics*, edited by the Commission of the European Communities, DG XIII/F AIM. Proceedings of the AIM Working Conference, Brussels, 19-21 March 1990, IOS Press, 1991.

[2] Commitee on Maintaining Privacy and Security in Health Care Applications of the National Information Infrastructure, *For the Record: Protecting Electronic Health Information,* National Academy Press, 1997.

[3] J. A. Cooper, *Computer and Communication Security*, Mc Graw Hill, 1989.

[4] W. Ford, *Computer Comunication Security: principles, standard protocols and techniques*, Prentice-Hall 1994.

[5] B. Schneier, *Applied Cryptography*, John Wiley, 1996.

[6] C. Hare e K. Siyan, *Internet Firewall and Network Security*, New Riders Publishing, 1996.