



TELEMED



TELEMED SICUREZZA

Indice

- Autenticazionepag 2
- Trasmissione dati tra client e server.....pag 3
- Salvataggio dati nel database.....pag 4
- Riferimenti.....pag 5

Il servizio Telemed è stato implementato con livelli di sicurezza medio-alti.

La sicurezza dei dati viene gestita a diversi livelli, tra cui **l'autenticazione, la trasmissione dei dati tra client e server, ed il salvataggio dei dati nel database**

Autenticazione:

L'autenticazione viene garantita da un sistema di login, studiato in modo tale da prevenire tentativi di intrusione di diverso tipo.

Il sistema di login si basa sull'uso dell'algoritmo di codifica non reversibile MD5, implementato sul client tramite javascript per prevenire un tentativo di sniffing dati del tipo "man in the middle".

Il problema fondamentale nei sistemi di login tradizionali è la possibilità per un utente esterno di intercettare il traffico dati tra il client e il server, nel tentativo di recuperare la password che solitamente viene trasmessa in chiaro, benchè poi sia immagazzinata nel database codificata.

Questo è il punto debole classico della fase di login, che questo sistema riesce a correggere:

- Ogni tentativo di login è legato ad un challenge alfanumerico casuale, che viene spedito al cliente una volta generato dal server.
- Quando l'utente digita username e password, la password viene codificata tramite l'algoritmo MD5 dopo essere stata concatenata al challenge: il risultato viene codificato con MD5 una seconda volta per ulteriore sicurezza.
- Quanto generato viene passato al server, insieme al challenge, che lo confronta con i dati contenuti nel database: se i campi inseriti sono corretti, viene rilasciato un cookie codificato con l'algoritmo RIJNDAEL a 256 bit
- Per prevenire attacchi a forza bruta sulla stringa codificata con MD5 (l'attacco è comunque materialmente impossibile, vista la potenza di calcolo necessaria per de-codificare una stringa codificata con due passaggi MD5), ogni challenge ha una vita massima configurabile (di default 5 minuti).
- Viene inoltre verificata la corrispondenza tra il numero di IP di chi effettua l'apertura della pagina di login, e di chi inserisce effettivamente i dati di accesso.

Trasmissione dati tra client (tipicamente il browser dell'utente) e server

La trasmissione dati viene garantita dal protocollo SSL a 128 bit e da un certificato di sicurezza emesso da un ente autorizzato.

Cosa significa SSL?

Secure Sockets Layer (SSL) è un protocollo sviluppato da Netscape che permette di proteggere l'informazione che passa tra client e server. Attraverso l'uso di tecniche crittografiche come la codificazione e la firma digitale, questo protocollo rende possibile le seguenti funzioni:

- Permette ai browser e server del Web di autenticarsi a vicenda
- Fa sì che informazioni confidenziali possano essere scambiate tra browser e server, senza che siano accessibili a terzi
- Assicurano che gli scambi dei dati tra browser e server non possano essere alterati, in maniera accidentale o intenzionale

Certificati di sicurezza

Le chiavi (keys) che stabiliscono delle connessioni sicure tramite i protocolli SSL si chiamano certificati di sicurezza.

Un certificato pubblico di sicurezza è analogo a un passaporto nel senso che dimostra l'identità di un soggetto ed è autorizzato da un terzo organismo conosciuto nel mondo della sicurezza come Certification Authority (CA). Questo organismo certificatore può essere paragonato a un Ufficio Passaporti: verifica l'identità, crea un documento riconosciuto e valido, e rilascia il documento stesso.

Autorità di Certificazione

Un'Autorità di Certificazione è un'autorità accreditata, responsabile dell'emissione dei certificati utilizzati per l'identificazione di una comunità d'individui, di sistemi o di altre identità che utilizzano una rete informatica.

Firmando in modo digitale i certificati emessi, l'Autorità di Certificazione unisce l'identità del possessore del certificato ad una chiave d'accesso all'interno del certificato stesso, facendosi così garante della validità di quest'ultimo. Coloro che utilizzano il network possiedono la chiave e la usano per verificare certificati di altri. Così facendo hanno la sicurezza che questi certificati siano autentici e che si riferiscano alla persona in questione, e sanno che

L'Autorità di Certificazione quale organo di fiducia si farà garante di questa certificazione. L'Autorità di Certificazione ha un ruolo cruciale nella sicurezza del Web e fa in modo che la certificazione per conto terzi sia possibile.

In un sistema di network complesso quale il Web, il modello di fiducia per conto terzi è necessario nelle numerose e dinamiche relazioni tra client e server. È possibile che i server e i client non abbiano stabilito un rapporto di fiducia reciproca; in ogni caso entrambe le parti hanno interesse ad avere trasmissioni sicure.

L'Autorità di Certificazione è l'anello mancante che permette trasmissioni sicure. Avendo garanzie dall'Autorità di Certificazione e dato che questo organismo ha inoltre garantito per l'identificazione e validità di entrambe le parti, la transazione di dati può avvenire senza rischi di frode e con assoluta sicurezza.

Salvataggio dati nel database

I dati sensibili vengono salvati sul database in forma criptata, tramite un nuovo algoritmo molto sicuro, Rijndael a 256 bit.

Per criptare, la stringa viene passata tramite un algoritmo di hash SHA1 (Secure Hash Algorithm versione 1.0), in modo da ottenere una verifica della lunghezza della stringa stessa (checksum).

La lunghezza viene posta all'inizio della stringa in modo da migliorare la codifica grazie alla sua natura pseudo casuale e perchè ha lunghezza nota.

Anche la chiave viene passata tramite SHA1, in modo da renderla più sicura (ed evitare un attacco alla password tramite dizionari).

Un vettore di inizializzazione viene quindi generato, in modo da essere accodato al testo cifrato.

Infine avviene la criptazione vera e propria, eseguita tramite il vettore di inizializzazione con l'algoritmo Rijndael a 256 bit.

Riferimenti

Algoritmo SHA1 (Secure Hash Algorithm versione 1.0)

B. Schneier. Applied Cryptography : Protocols, Algorithms, and Source Code in C. Wiley, 2nd Edition, 1995.

B. Preneel. Analysis and Design of Cryptographic Hash Functions. Ph.D. Thesis, Katholieke University Leuven, 1993.

M.J.B. Robshaw. MD2, MD4, MD5, SHA and Other Hash Functions. Technical Report TR-101, version 4.0, RSA Laboratories, July 1995.

http://www.w3.org/PICS/DSig/SHA1_1_0.html

Algoritmo Rijndael

<http://csrc.nist.gov/encryption/aes/rijndael/>

<http://www.esat.kuleuven.ac.be/~rijmen/rijndael/>

SSL

R. Rivest, A. Shamir, and L. M. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Communications of the ACM, v. 21, n. 2, Feb 1978, pp. 120-126.

<http://wp.netscape.com/eng/ssl3/>