
SICUREZZA INFORMATICA
E NORMATIVA

Protocollo set:

È il più efficiente protocollo nato per la protezione dei dati nel mondo dell' e-commerce. Sviluppato congiuntamente da visa e mastercard .

Alla sua efficienza si affianca però una difficile implementazione che ne ha limitato l'utilizzo.

Infatti per poter essere utilizzato si richiede il ritiro da parte dell'utente con il rilascio di un dispositivo software plug in su memoria di massa in singola copia .

Quando l'utente effettua un pagamento il software interagisce con il server del rivenditore che a sua volta contatta un server certificatore per verificare se l'utente sia possessore della carta di credito se c'è una conferma il pagamento verrà effettuato

Il meccanismo può funzionare anche in senso inverso e cioè il set garantisce l'identità del rivenditore all' utente così avrà conferma del suo acquisto.

I protocolli https e ssl:

Il sistema attualmente più utilizzato per le transazioni online è il protocollo SSL (secure socket layer) , con il tempo è divenuto uno standard per le transazioni online anche quelle che richiedono un alto tasso di sicurezza. Esso è inserito tra i protocolli del TCP\IP e insieme all' HTTP forma il protocollo HTTPS. Il protocollo provvede alla sicurezza del collegamento attraverso tre funzionalità fondamentali :

1. Privacy del collegamento: dopo una sincronizzazione iniziale tra mittente e destinatario i dati vengono crittografati tramite crittografia asimmetrica
2. Autenticazione l'identità viene autenticata tramite crittografia asimmetrica avendo così la certezza di comunicare con il giusto server
3. Affidabilità : il livello di trasporto include un controllo dell'integrità del messaggio in tal modo si verifica se i dati non sono stati alterati durante la trasmissione

Funzionamento del protocollo https per stabilire una connessione sicura

1. Il browser richiede il certificato e invia una lista di algoritmi di cifratura
2. Il web server invia il certificato e gli algoritmi di cifratura utilizzati
3. Il browser convalida il certificato
4. Genera la chiave di sessione per la crittografia asimmetrica
5. Cifra la chiave di sessione utilizzando la chiave pubblica del server presente nel certificato
6. Il browser invia la chiave di sessione cifrata
7. Il web server decifra la chiave utilizzando la sua chiave privata
8. Infine invia un acknowledge .


SICUREZZA
NELL'
E-COMMERCE

Sicurezza nell'e-commerce:

- **Sicurezza dei dati**: considera le tracce che l'utente lascia negli acquisti online;
- **Sicurezza nei traferimenti**: riguarda problemi legati ad **autenticazione**, **trasferimento** e **conservazione** dei dati relativi alle carte di credito.

Principali truffe nell'e-commerce:

- Vendita di prodotti da siti civetta;
- Realizzazione di siti clonati;
- Aziende fallimentari accumulanti ordini.

I sistemi più diffusi per garantire la sicurezza nei dati e nei pagamenti sono il **protocollo SSL** e il **protocollo SET**.

Funzionamento di un acquisto online:

→ ACCESSO AD UN NEGOZIO VIRTUALE SU SITO INTERNET

→ ORDINE DI ACQUISTO

→ RICHIESTA DI AUTORIZAZZIONE

Le parti coinvolte in una transazione commerciale sono:

1. **Acquirente;**
2. **Venditore;**
3. **Ente finanziario;**
4. **Gateway di pagamento;**
5. **Società emittente;**
6. **Authority.**

Esempio acquisto online:

Il signor Rossi sta effettuando un acquisto dal sito www.mondadorieducation.it attraverso una carta di credito emessa dalla Società Z. www.mondadorieducation.it si appoggia all'ente finanziario Ente Y.

1. Una volta confermato l'ordine, entra in azione il gateway di pagamento;
2. Si crea un collegamento protetto tra il sito www.mondadorieducation.it e l' Ente Y, al cui interno il signor Rossi digiterà i suoi dati personali e il suo numero di carta di credito che viene registrato dal server sicuro dell' Ente Y;
3. L' Ente Y inoltra la richiesta di autorizzazione al pagamento ai circuiti internazionali e alla Società Z;
4. I circuiti internazionali comunicano all' Ente Y l'esito della richiesta;
5. L' Ente Y comunica tale esito sia al signor Rossi che a www.mondadorieducation.it;
6. L'acquisto è concluso, la conferma viene comunicata tramite e-mail.

I C  KIE E LA SICUREZZA

Cosa sono?

I cookie (biscotto) sono piccoli file di testo che i web server creano e memorizzano sui computer dei visitatori per poterli identificare nelle visite successive o,più in generale, per archiviare sul client informazioni utili al server.
Questi piccoli pezzi d'informazione vengono inviati dal web server al browser quando questo si connette per la prima volta .In seguito ,il browser rinvierà una copia del cookie al server all'inizio di ogni connessione.

I cookie:
Bene o Male?

Inizialmente sono stati creati per facilitare la navigazione sul web,aiutandoci a memorizzare informazioni come nominativi e password,per poi rendere più fruibile l'entrata in determinati siti,o anche per memorizzare le nostre ricerche e i nostri interessi ,così da indirizzarci verso ciò che ci poteva essere di aiuto . Ma proprio questi fattori che li resero così importanti per la nostra navigazione,diventarono fonte di ispirazione per fare promozioni mirate ,o ancora peggio per rubare dati sensibili come quelli elencati in precedenza .

Poiché possono essere usati per monitorare la navigazione su Internet, i cookie sono oggetto di discussioni concernenti il diritto alla privacy. Molti paesi ed organizzazioni, fra cui gli Stati Uniti e l'Unione europea, hanno legiferato in merito. I cookie sono stati inoltre criticati perché non sempre sono in grado di identificare l'utente in modo accurato ed inoltre perché possono potenzialmente essere oggetto di attacchi informatici. Esistono alcune alternative ai cookie, ma tutte, insieme ad alcuni vantaggi, presentano controindicazioni.

I cookie vengono spesso erroneamente ritenuti veri e propri programmi e ciò genera errate convinzioni. In realtà essi sono semplici blocchi di dati, incapaci, da soli, di compiere qualsiasi azione sul computer. In particolare non possono essere né spyware , né virus. Ciononostante i cookie provenienti da alcuni siti sono catalogati come spyware da molti prodotti anti-spyware perché rendono possibile l'individuazione dell'utente. I moderni browser permettono agli utenti di decidere se accettare o no i cookie, ma l'eventuale rifiuto rende alcuni oggetti inutilizzabili. Ad esempio, gli shopping cart implementati con i cookie non funzionano in caso

Com’è fatto un cookie?

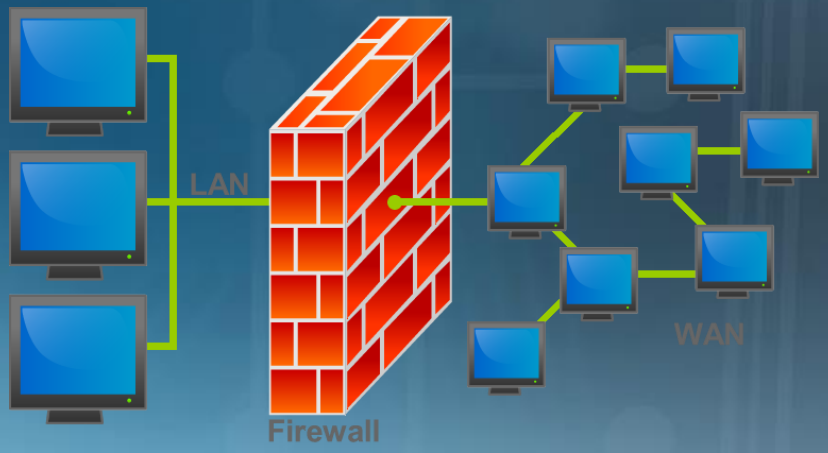
I cookie contengono queste specifiche caratteristiche che fanno in modo di verificare se la persona che ne vuole fare uso sia realmente autorizzata:

- L’identificatore di sessione (session ID),per informazioni inerenti a varie autorizzazioni;
- L’ora e la data in cui il cookie è stato rilasciato;
- La data di scadenza del cookie;
- L’indirizzo IP del browser al quale il cookie è stato rilasciato;
- Un messaggio di autenticazione (codice MAC).

Insieme a tutto ciò per identificare un cookie gli viene attribuita una coppia nome/valore (considerata una variabile),una data di scadenza non indicata (dopo il periodo di tempo prestabilito il cookie viene eliminato automaticamente),ed a ogni cookie viene associato un Dominio ed un Percorso con i quali vengono stabiliti i cookie validi per il sito in cui si sta navigando.

IL FIREWALL:

In informatica, un **firewall** è un componente passivo di difesa perimetrale di una rete informatica, che può anche svolgere funzioni di collegamento tra due o più tronconi di rete, garantendo dunque una protezione in termini di sicurezza informatica della rete stessa. Di norma, la rete viene divisa in due sottoreti: una, detta esterna, comprende interamente Internet mentre l'altra interna, detta LAN In alcuni casi è possibile che nasca l'esigenza di creare una terza sottorete detta DMZ (o zona demilitarizzata) adatta a contenere quei sistemi che devono essere isolati dalla rete interna, ma che devono comunque essere protetti dal firewall ed essere raggiungibili dall'esterno.



Definizione e funzionalità:

DEFINIZIONE: Apparato di rete hardware o software di ingresso-uscita bidirezionale che, opportunamente configurato o settato e agendo in maniera centralizzata, filtra tutti i pacchetti entranti ed uscenti, da e verso una rete o un computer, secondo regole prestabilite che contribuiscono alla sicurezza della stessa.

Un *FIREWALL* può essere :

- *Un semplice computer con due schede di rete (una per l'input e l'altra per l'output) con un software adatto.*
- *Una funzionalità logica (software)inclusa su un router o su un apparato hardware dedicato.*

Esistono anche "firewall personali" che sono programmi installati sui normali computer che filtrano solamente i pacchetti che entrano ed escono da quel calcolatore utilizzando una sola scheda di rete.

Funzionalità: Il firewall controlla tutti i pacchetti in entrata e in uscita dalla rete interna (LAN), effettuando delle operazioni:

- Controllo
- Modifica
- Monitoraggio

I TIPI DI FIREWALL:

Esistono diversi tipi di FIREWALL: (in ordine decrescente di complessità)

packet filter:

è il più semplice e si limita a valutare gli header di ciascun pacchetto, decidendo quali far passare e quali no sulla base delle regole configurate.

stateful inspection:

tiene traccia di alcune relazioni tra i pacchetti che lo attraversano, ad esempio ricostruisce lo stato delle connessioni TCP.

deep packet inspection:

effettuano controlli fino al livello 7 della pila ISO/OSI, ovvero valutano anche il contenuto applicativo dei pacchetti, ad esempio riconoscendo e bloccando i dati appartenenti a virus o worm noti in una sessione HTTP o SMTP.

application layer firewall:

sono apparati che intercettano le connessioni a livello applicativo. A questa categoria appartengono i proxy. In tali casi, la configurazione della rete privata non consente connessioni dirette verso l'esterno, ma il proxy è connesso sia alla rete privata che alla rete pubblica, e permette alcune connessioni in modo selettivo, e solo per i protocolli che supporta.

IL SERVER PROXY:

Un **proxy** è un *server* che agisce da intermediario in una connessione, ricevendo le richieste da un computer cliente e reindirizzandole verso altri server, destinatari delle richieste.

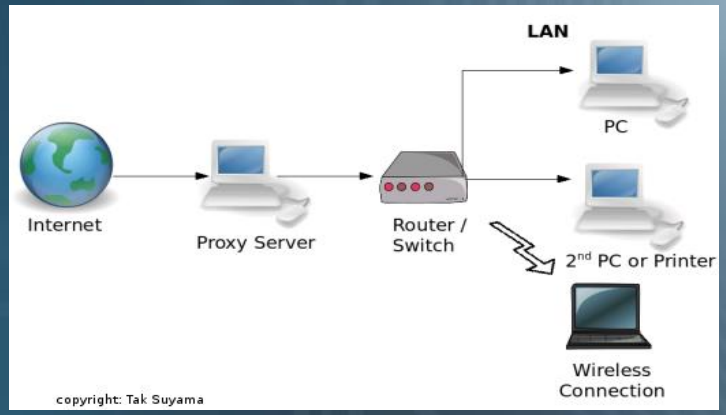
Come funziona:

Un proxy è un computer collegato alla Rete. Come tutti gli altri computer, si trova in un posto ben preciso, che ne determina la nazionalità

I motivi per utilizzare un proxy, invece di una normale connessione, sono molti.

Un proxy può essere usato per una o più delle seguenti ragioni:

- **Connettività**
- **caching**
- **Monitoraggio**
- **controllo**
- **Privacy**



Come si utilizza un proxy?

Come ogni altro computer connesso alla Rete (incluso il nostro), il proxy ha un **indirizzo IP,** che lo identifica e localizza. Se vogliamo collegarci a un proxy, dobbiamo conoscere il suo indirizzo IP e impostare il nostro browser, cioè il programma con cui navighiamo in internet, perché si conneta a quel proxy.

Application gateway:

Un **gateway** (dall'inglese, *portone*, *passaggio*) è un dispositivo di rete che opera al livello di rete e superiori del modello ISO/OSI. Il suo scopo principale è quello di veicolare i pacchetti di rete all'esterno di una rete locale (LAN)

Gateway è un termine generico che indica il servizio di inoltro dei pacchetti verso l'esterno; il dispositivo hardware che porterà a termine questo compito è tipicamente un router. Nelle reti più semplici è presente un solo *gateway* che inoltra tutto il traffico diretto all'esterno verso la rete Internet. In reti più complesse in cui sono presenti parecchie subnet, ognuna di queste fa riferimento ad un *gateway* che si occuperà di instradare il traffico dati verso le altre sottoreti o reindirizzarlo ad altri *gateway*.

Spesso i *gateway* non si limitano a fornire la funzionalità di base di *routing*, ma integrano altri servizi da e verso la rete locale come proxy DNS, firewall, NAT etc, che sono appunto servizi di strato di rete più elevato ovvero applicativo.

Principio di funzionamento del gateway:

Un computer connesso alla rete locale confronta i primi bit dell'indirizzo di destinazione dei dati da inviare (quelli che corrispondono ai bit settati a "1" nella sua subnet mask) con il network prefix (già noto) del proprio indirizzo IP:

- se corrispondono, significa che il computer di destinazione è sulla stessa rete locale;
- se invece non corrispondono, il computer d'origine invia i dati al *gateway* predefinito, il quale si occuperà del loro successivo instradamento verso la rete remota di destinazione.
- non possono coesistere in una stessa rete 2 computer con lo stesso indirizzo IP (conflitto IP; il secondo arrivato disattiva la propria scheda di rete).

La sicurezza del cloud computing:

Il cloud computing è uno dei cambiamenti più significativi nell'information technology infatti in futuro saranno sempre meno i computer con hard disk e i dati saranno memorizzati su una nuvola, questo futuro è in parte già presente grazie a sistemi come Google Chrome e Windows 8… questa tecnologia può semplificarci tantissimo la vita.
Attraverso i servizi di una piattaforma cloud un utente può accedere ad una architettura condivisa e configurabile di risorse : server, CPU, memoria RAM applicazioni. Però le architatture cloud non sono tutte uguali ad oggi infatti esistono due modelli di cloud : i modelli di servizio ed i modelli di erogazione.
I modelli di servizio evidenziano le caratteristiche essenziali che dimostrano la loro relazione e le loro differenze rispetto agli approcci tradizionali al cloud computing.
Infrastructure as a service (Iaas): le funzionalità offerte comprendono capacità computazionale, storage, connettività ed altre componenti con la quale un cliente può installare e gestire un software tuttavia ha il controllo del solo sistema operativo senza controllare l'infrastruttura sottostante.
Platform as a service (Paas): le funzionalità offerte permettono di gestire delle applicazioni compatibili con la piattaforma ma in questo caso il cliente gestisce solo le applicazioni installate.
Software as a service (SaaS): le funzionalità offerte sono quelle delle applicazioni, in questo caso il cliente gestisce solo alcune limitate configurazioni dell' applicazione.

I modelli di erogazione:

Questo tipo di modelli cloud emergono in seguito alla maturazione delle offerte sul mercato e della domanda dei clienti

❖Cloud pubblico: questo modello prevede l'erogazione aperta e condivisa dei servizi di cloud computing ad un ampio numero di utenti, il cloud pubblico risulta ottimo per le aziende e le piccole realtà che necessitano di un numero ristretto di applicazioni tuttavia ci sono alcune riserve riguardo la gestione dei dati e la loro sicurezza visto che i dati vengono salvati in un cloud al di fuori dell' azienda

❖Cloud privato: è un sistema che consente di mantenere i dati all' interno della struttura operativa con ovvi vantaggi per quanto riguarda la gestione e la sicurezza inoltre da la possibilità di usufruire con un sistema semplificato configurabile ed efficiente

❖Cloud ibrido: è un infrastruttura ibrida che consente di utilizzare i vantaggi del cloud pubblico e la sicurezza del cloud privato. Esso viene scelto da aziende che vogliono costruire un sistema interno ma allo stesso tempo usufruire di un sistema pubblico per la gestione dei dati.
Gli unici aspetti negativi del cloud sono legati per lo più all' aspetto della sicurezza

CLOUD E SICUREZZA: CLIENTE E FORNITORE

Il CLIENTE:

- Il cliente nei modelli Iaas e PaaS deve:

Verificare i servizi inutili, le opzioni di default ed eventuali backdoor del fornitore;
Installare sistemi per monitorare le prestazioni del sistema (ram, banda di rete, cpu)

- Il cliente nei modelli SaaS deve:

Accertarsi della sicurezza applicativa garantita dai servizi SaaS,
Verificare le modalità di controllo accessi;
Verificare i profili disponibili.

- Il cliente in tutti i modelli deve effettuare un sistema di backup senza basarsi su quello offerto dal fornitore (basato sulle prestazioni offerte dal fornitore e deve essere testato)

IL FORNITORE:

Cosa deve fare il fornitore:

- Politica per la sicurezza e direzione aziendale;
- Stabilire ruoli e responsabilità;
- Occuparsi della formazione sulle tecnologie specifiche;
- Occuparsi delle relazioni tra vendita e produzione;
- Occuparsi delle relazioni tra fornitore e cliente;
- Scegliere i prodotti;
- .
- Evitare la proliferazione delle macchine;
- Standardizzare procedure e best practice;
- Chiarire procedure e tecniche di processo.
- Gestire cambiamenti di configurazioni in modo controllato

In un ambiente cloud, una maggiore quantità di dati viene condivisa con diversi client in rete, per questo motivo la sicurezza diventa ancora più vitale ai fini della protezione. La crittografia è uno strumento che offre proprio i vantaggi di affidamento minimo per il fornitore di servizi Cloud.
Si parlerà di:

Encrypting data in transit over networks: vi è la necessità di crittografare le credenziali multi-uso, come ad esempio numeri di carte di credito, password e le chiavi private, in transito su Internet.

Encrypting data at rest: si intende la crittografia dei dati su disco o in un database di produzione in tempo reale, come si può proteggere contro un fornitore di servizi Cloud dannoso o maligno.

Esistono anche sistemi crittografici che permettono di verificare in maniera automatica se il cloud provider stia memorizzando tutti i dati archiviati per anni, senza doversi ricordare tutto il contenuto.

Per quanto riguarda la sicurezza in rete, la tranquillità del trasporto delle informazioni è garantita tramite il protocollo https (hyper text transfer protocol secure). HTTPS è un protocollo che integra l'interazione del protocollo HTTP attraverso un meccanismo di crittografia di tipo Transport Layer Security(SSL/TLS). Per impostare un web server in modo che accetti connessioni di tipo HTTPS, l'amministratore di rete deve creare un certificato digitale ovvero un documento elettronico che associ l'identità di una persona ad una chiave pubblica. In particolari situazioni (come per esempio nel caso di aziende con una rete intranet privata) è possibile avere un proprio certificato digitale che si può rilasciare ai propri utenti. Questa tecnologia quindi può essere usata anche per permettere un accesso limitato ad un web server. L'amministratore spesso crea dei certificati per ogni utente che vengono caricati nei loro browser contenenti informazioni come il relativo nome e indirizzo e-mail in modo tale da permettere al server di riconoscere l'utente nel momento in cui quest'ultimo tenti di riconnettersi senza immettere nome utente e/o password.
I servizi in cloud devono consentire la verifica della sicurezza dei dati sensibili, inoltre assicurano la **business continuity** e il **disaster recovery**, grazie alla possibilità di effettuare backup.

Le principali certificazioni che permettono ad un sistema di essere classificato come sistema di gestione della sicurezza delle informazioni sono : ISO/IEC 27001, SAS Type II Audit e BS25999