

E-Commerce & Security



Angelico Massimo – 823903

Corso di E-commerce
anno accademico 2011
Professore : Marek Maurizio

Argomenti trattati

- Sistemi di pagamento
- Protocolli per la sicurezza transazioni
- Principali attacchi informatici
- Truffe
- Esempi reali
- Conclusioni

Introduzione

- Lo sviluppo del commercio on-line ha portato all'implementazione di nuovi sistemi di pagamento che hanno così determinato il passaggio dalla banconota cartacea al "contante digitale".
- I fondamentali vantaggi connessi all'utilizzo dei metodi di pagamento on-line sono rappresentati dalla convenienza e dall'efficienza che li caratterizzano.

Sviluppo tecnologico, accesso rapido al web, dispositivi mobile hanno favorito i pagamenti nel mondo telematico rendendo estremamente facile tale servizio.

Sistemi di pagamento 1 di 2

❑ **Carta di Credito**

Il principale metodo di pagamento per le transazioni on-line

Il cliente invia al venditore gli estremi della carta di credito.

Il venditore verifica i dati trasmettendoli alla banca.

Le transazioni vengono addebitate sul conto corrente in via posticipata.

❑ **Bonifico Bancario**

Conclusa la transazione il venditore comunica gli estremi bancari ai quali effettuare un bonifico per pagamento merce. Al ricevimento del bonifico l'esercente invia la merce.

❑ **Contrassegno**

Questa forma di pagamento consente al cliente di correre il rischio minore, poiché il pagamento viene effettuato solo una volta che la merce è giunta a destinazione.

Sistemi di pagamento 2 di 2

❑ **PayPal**

E' la società del gruppo eBay che consente a chiunque possieda un indirizzo e-mail di inviare o ricevere pagamenti online.

Metodo alternativo alla carta di credito. Garantisce anonimato delle parti

❑ **Carte Prepagate**

Carte che si possono acquistare con un importo disponibile prefissato ed eventualmente anche ricaricarle. Inoltre, in caso di abusi, siamo sicuri che il danno subito non potrà superare il valore della carta prestabilito.

Utilizzate per piccoli acquisti in Internet

❑ **PaySafeCard**

L'utente acquista in un punto di vendita un credito che gli viene messo a disposizione in forma di un PIN con 16 numeri. Questo PIN viene indicato durante un pagamento in un webshop. Se il credito della Paysafecard è esaurito, il rispettivo PIN diventa invalido e l'utente deve acquistare una nuova Paysafecard. [Senza dati personali o coordinate bancarie]

PaySafeCard



1. Acquista la paysafecard in un punto vendita del taglio desiderato.
 2. Riceverai paysafecard sotto forma di scontrino con un codice PIN a 16 cifre da immettere nel web shop desiderato.
 3. Al momento del pagamento inserisci il codice PIN
- Per pagamenti consistenti è possibile accorpare fino a 10 PSC.
 - Puoi pagare anche in valuta straniera
 - Se il credito della Paysafecard è esaurito, il rispettivo PIN diventa invalido

Oltre al principio di Prepaid dove non sono necessari i dati personali, la PSC offre tramite l'inerente procedura Prepaid quasi una tutela completa dalla truffa come per esempio il furto d'identità.

SICUREZZA

- Uno dei problemi più sentiti nel mondo dell' e-commerce è indubbiamente la sicurezza nelle modalità di pagamento.
- Ad oggi, le modalità più diffuse sono il Prepaid, il contrassegno e il pagamento con la carta di credito, sicuramente il più interessato da questo problema.
- Inizialmente, il trasferimento delle informazioni personali tra venditore e cliente avveniva in chiaro costituendo un enorme problema per la sicurezza, in quanto i dati trasferiti potevano essere intercettati e quindi utilizzati da terzi.
- Oggi, questa pratica di trasferimento dei dati è stata sostituita a favore di pratiche più sicure che garantiscono una maggiore riservatezza delle informazioni personali.

Protocolli per le transazioni 1 di 4

I principali protocolli utilizzati nelle transazioni sicure.

➤ **SSL (*Secure Sockets Layer*)**

- Stabilisce un canale di comunicazione sicuro tra un browser ed un server;
- Implementato da Netscape Communications.
- Predecessore di TLS (*Transport Layer Security*) che è stato creato dal merge tra SSL e PCT (*Private Communication Technology*), quest'ultimo sviluppato dalla Microsoft.
- La componente fondamentale di una connessione protetta dal SSL è rappresentata dal SSL Handshake Protocol caratterizzato da una fase di negoziazione tra le parti e successivamente alla fase di trasferimento dei dati.

Se il server non può essere autenticato, la connessione non può essere stabilita

Protocolli per le transazioni 2 di 4

I principali protocolli utilizzati nelle transazioni sicure.

❑ **SET (Secure Electronic Transaction)**

- Il titolare della carta di credito SET riceve dalla banca emittente un certificato criptato che permette di identificare l'utente. Il titolare registra sul suo computer il certificato e, nel momento in cui effettua un pagamento via internet, dà la possibilità alla banca di certificare al venditore se chi sta utilizzando la carta sia l'effettivo titolare della stessa.
- La banca si sostituisce al venditore nell'onere di verificare la corrispondenza tra la firma di chi effettua il pagamento e la firma apposta sul retro della carta di credito.
- La transazione mette in gioco non soltanto l'acquirente e il venditore, ma anche le loro rispettive banche.
- Protegge l'identità di tutte le parti coinvolte nella transazione attraverso la firma digitale (crittografia a chiave pubblica) che permette di verificare il mittente ed il destinatario.

Protocolli per le transazioni 3 di 4

□ HTTPS

- Protocollo di livello applicativo
- Utilizzato per aggiungere sicurezza alle pagine del WWW in modo tale da rendere possibili applicazioni quali il commercio elettronico.
- E' costituito abbinando SSL al normale standard HTTP.
- Garantisce l'invio delle informazioni personali sottoforma di pacchetti criptati.
- Gli accessi vengono effettuati sulla porta 443 e tra il protocollo TCP e HTTP si interpone un livello di crittografia/autenticazione
- ForceTLS : add-on per Firefox (Facebook)

Protocolli per le transazioni 4 di 4

□ HTTPS

➤ Questo protocollo assicura una buona protezione contro attacchi del tipo man in the middle(attacco dell'uomo in mezzo).

E' un tipo di attacco nel quale l'attaccante è in grado di leggere, inserire o modificare a piacere, messaggi tra due parti senza che nessuna delle due sia in grado di sapere se il collegamento che li unisce reciprocamente sia stato effettivamente compromesso da una terza parte.

➤ Esiste una tecnica molto nota, chiamata ARP poisoning(*avvelenamento dell'ARP*) che rende gli attacchi "man in the middle" facilmente fattibili. Usando questa tecnica un malintenzionato riesce ad ingannare i PC presenti su una LAN facendogli pensare che una certa macchina, ovviamente controllata da un malintenzionato, funzioni da gateway locale , il che significa che tutti gli utenti della LAN gli invieranno a loro insaputa tutto il traffico Internet.

Principali attacchi on-line 1di2

➤ **Phishing**

Tecnica più diffusa per il furto di identità.

Si basa sull'utilizzo delle comunicazioni elettroniche, specie messaggi di posta elettronica falsi che hanno lo scopo di reperire credenziali dell'utente direttamente o attraverso link di siti fittizi.

Suo sostituto è il Vishing che si basa sulla comunicazione vocale come mezzo per spillare info sensibili.

➤ **Negazione del servizio (DoS)**

Condotto attraverso reti (botnet) formate da alcuni computer cosiddetti zombie, che connettendosi contemporaneamente ad un sito Internet lo sovraccaricano rendendolo inutilizzabile. Ancor più distruttivo è l'attacco distribuito su larga scala DDoS dove i computer attaccanti sono migliaia.

Questa tipologia di attacco viene normalmente utilizzata per scoprire falle nei siti di e-commerce, in modo da recuperare informazioni sugli utenti che si collegano, in particolare le credenziali d'accesso e numero di carte di credito.

Principali attacchi on-line 2di2

➤ **Keylogging**

Strumento in grado di intercettare tutto ciò che un utente digita sulla tastiera del proprio computer.

I keylogger possono essere hardware (collegati al cavo di comunicazione tra la tastiera ed il computer o all'interno della tastiera) o software (programmi che controllano e salvano la sequenza di tasti che viene digitata da un utente).

➤ **Firesheep**

E' un add-on per Firefox in grado di rendere estremamente facile il furto di identità. Cattura le credenziali di accesso degli utenti presenti su una stessa rete, e con un semplice login il cookie corrispondente viene catturato e lo mette a disposizione per l'accesso in una comoda barra laterale del browser. Sfrutta alcuni bug presenti nei siti web, quali Facebook, Amazon, Twitter

Firesheep



Truffe on-line

- Una truffa online avviene principalmente attraverso l'invio di e-mail e collegamenti a siti fasulli.
- Per quanto riguarda le e-mail, il loro obiettivo principale è quello di rubare la coppia user-password all'utente, in particolare le credenziali di servizi bancari presenti sul web.
- Altre tipologie di truffe hanno a che fare con i siti di e-commerce, dove il truffatore basta che crei un sito web con dati false e inizi a vendere prodotti a prezzi molto vantaggiosi. Questo tipo di sito nasconde un cosiddetto negozio fantasma, in quanto, dopo aver acquistato il prodotto questo non viene mai spedito e il negozio sparisce.
- Passaggio dal famoso pacco napoletano alle truffe sul web (Napoli detiene il record delle frodi su internet e dei furti d'identità).
- Numero delle denunce alla polizia postale per reati telematici è salito a circa 3mila, il 30% in più rispetto agli anni scorsi.

Esempi reali 1di2

○ Hack EMV

Un giovane studente dell'Università di Cambridge (Omar S. Choudary), presentando una tesi con tanto di video dimostrativo, ha mostrato come sia possibile utilizzare una carta di credito rubata sfruttando le falle presenti nella tecnologia "chip & pin" (basata sul protocollo EMV). La Smart Card Detective avrebbe varie funzionalità e fornirebbe in tempo reale alcune informazioni sulla transazione, permettendo al titolare della carta di controllare che la somma visualizzata sul POS di un dato esercizio commerciale sia effettivamente quella addebitatagli e che il terminale non sia stato di fatto alterato.



Esempi reali 2di2

○ Truffa su Facebook

- L' applicazione che permette di giocare online a Twilight Breaking Dawn è una truffa.
- Iniziando a giocare, automaticamente viene deciso che il gioco "vi piace", esponendo così al pericolo anche tutti gli amici. In più viene permesso a "terze parti" di accedere al vostro account e sarà fornito anche un sondaggio "malevolo" da compilare.



Conclusioni

- Con la diffusione dell'e-commerce si sono diffuse truffe sempre più insidiose che colpiscono principalmente gli acquirenti.
- Si passa dalla vendita di prodotti da siti civetta dove al ricevimento del pagamento non viene inviata la merce, o viene solamente simulata la spedizione alla realizzazione di siti clonati con la finalità di rubare informazioni quali il codice della carta di credito.
- Esistono appositi plug-in per Firefox, esempio Netcraft toolbar, che blocca l'accesso a siti truffaldini.
- Prima di effettuare un pagamento online, in particolar modo su un venditore non conosciuto, bisogna prima di tutto verificare se nel sito sono presenti la partita IVA e riferimenti quali il numero di telefono e l'indirizzo fisico che permettono di contattare l'azienda.
- In secondo luogo, verificate che il negozio on-line permetta altre forme di pagamento oltre alla carta di credito, per esempio la vendita in contrassegno. Cercare informazioni sul venditore utilizzando i motori di ricerca.