Codici delle carte di credito e formula di Luhn

Giulio Galanello & Jessica Cerquetelli

1 Introduzione

In questa relazione abbiamo preso in esame i codici numerici presenti in una qualsiasi carta di credito moderna. Dopo una breve introduzione in cui abbiamo trattato gli aspetti generali di quest'ultime, ci siamo concentrati sulle varie tipologie di codici numerici presenti in esse. In particolare abbiamo analizzato il codice identificativo e la relativa cifra di controllo descrivendo uno degli algoritmi più utilizzati oggi, quello di Luhn. Infine ci siamo occupati del 3d-secure del fenomeno del keylogger.

2 Generalità sulle carte di credito

La carta di credito, o "*moneta elettronica*", è uno strumento di pagamento rilasciato da una banca o da un ente finanziario. Inizialmente esse erano dotate unicamente di una banda magnetica collocata sul retro, successivamente per motivi di sicurezza venne aggiunto anche un microchip,rendendola così una "*smart-card*".Il sistema di funzionamento delle carte di credito è un processo di autorizzazione del sistema bancario. Questo processo si articola in tre soggetti:ente emittente, ente esercente, circuito di pagamento. L'ente emittente (*issuer*) che può essere una banca oppure un ente finanziario è l'azienda che provvede a emettere la carta di credito. L'ente esercente (*merchant*) è l'esercizio commerciale che permette ai propri clienti il pagamento mediante carta di credito. Il circuito di pagamento è l'azienda che si occupa di selezionare le domande e le corrispondenti autorizzazioni alla spesa. La rete del circuito si allarga attraverso la delega agli "*acquirer*" a installare i POS (*point of sale)* ovvero i dispositivi adibiti ai pagamenti elettronici.La carta di credito è, quindi, uno strumento che consente di regolare il pagamento successivamente all'acquisto. Tra i principali circuiti di pagamento ricordiamo:Visa,MasterCard, American Express, Diners e Discover Card. Le carte di credito si dividono in tre tipologie:carte di credito a saldo, carte *revolving* e carte *co-branded.* La carta a saldo è il genere attualmente più diffuso in Italia ed è solitamente associata

ad un conto corrente bancario. Permette di pagare entro 45 giorni la merce acquistata senza alcun costo aggiuntivo. La carta *revolving* consente di rateare il pagamento del bene acquistato. La rateazione comporta un costo aggiuntivo per l'acquirente dovuto al saldo degli interessi sul finanziamento, entro un importo massimo detto fido. L'ultima tipo di carta, *co-branded*, funziona come una *revolving* ma viene emessa da una banca o ente finanziario in collaborazione con un azienda che ne facilita la diffusione presso i propri clienti.

3 Codici delle carte di credito

Iniziamo con il presentare i principali codici presenti in una carta di credito.

(1) *Il codice identificativo*

Presente sul dorso della carta è costituito da sedici cifre in rilievo che consentono di identificarla "completamente" .
Il primo numero rappresenta la tipologia della carta di credito ovvero il circuito a cui essa appartiene (3 per le American Express o le Diners, 4 per le Visa, 5 per le MasterCard e 6 per le Discover card). I numeri dalla seconda alla sesta cifra identificano la banca (tale codice viene detto BIN). Le cifre dalla settima alla quindicesima individuano il numero del conto corrente del proprietario. Infine la sedicesima è una cifra di controllo. Nella sezione successiva approfondiremo le questioni relative alla cifra di controllo ed agli errori.

(2) *La banda magnetica*

Si trova sulla parte posteriore di ogni carta ed è formata da tre differenti tracce sulle quali vengono immagazzinati dati di diverso tipo.La traccia che viene letta dai macchinari POS durante i pagamenti è la seconda della banda. Essa contiene quaranta caratteri numerici e a ciascuno di essi corrisponde una particolare tipologia di informazioni. Il primo carattere è solamente una sentinella (*start sentinel*) che precede i dati veri e propri. I successivi sedici caratteri, o meno, a seconda della tipologia di carta sono i caratteri identificativi della carta di credito. Dopo di questi è presente il simbolo "=" che ha la funzione di separatore. I quattro caratteri successivi danno

informazione sulla scadenza della carta di credito (il mese e l'anno). Segue il codice di servizio costituito da tre cifre (101 per le carte di credito e 121 per le carte di debito) e il pin crittografato. Chiudono la serie il simbolo e "?" e "=".

(3) *I codici di sicurezza.*

Questi codici costituiscono un'ulteriore misura di sicurezza nelle transazioni online con carta di credito e consentono all'istituto che ha emesso la carta, di verificare l'identità del titolare, prevenendo possibili frodi. Il nome e la posizione del codice di sicurezza sulla carta variano in relazione al circuito e alla banca che l'ha emessa. Nel caso delle carte American Express il numero di verifica è detto CVV (*Card Verification Value*) è composto da 4 cifre e si trova nella parte anteriore della carta, sopra il codice identificativo. Nelle carte di credito MasterCard e Visa ci sono due codici di sicurezza, entrambi denominati CVC (*Card Verification Code*). Il codice di sicurezza della carta di credito CVC 1, di tre cifre, è inserito nella banda magnetica, il codice CVC 2 è impresso sulla carta dove c'è la firma del titolare. In entrambi i casi la presenza dei codici è dovuta al tentativo di scoraggiare l'utilizzo fraudolento della carta da parte di terzi.

(4) *Il codice titolare carta di credito.*

Il numero (di solito di dieci cifre) riportato sull'estratto conto in alto è il codice titolare. Assieme al codice di sicurezza, il codice titolare serve per poter dare il via a delle operazioni o per richiedere dei servizi con la carta di credito. È opportuno, per ogni evenienza, tenere sempre a portata di mano il codice titolare ed il codice di sicurezza delle proprie carte di credito.

(5) *Il codice Pin.*

Il codice Pin della carta di credito è personale, permette di prelevare contanti presso gli sportelli automatici di tutto il mondo che fanno parte del proprio circuito e di effettuare pagamenti. Deve rimanere segreto.

4 Cifra di controllo ed errori

In informatica la rilevazione-correzione dell'errore ha una grande importanza pratica nel mantenimento dell'integrità dell'informazione dei dispositivi per l'immagazzinamento dei dati. La rilevazione dell'errore consiste nella capacità di scoprire la presenza di errori causati da fenomeni deterioranti durante una trasmissione di dati. La correzione è invece la capacità di ricostruire i dati originali eliminando quindi gli eventuali errori. Tale problema interessa ovviamente i codici identificativi delle carte di credito. Come già detto l'ultima cifra di un codice identificativo è una "cifra di controllo" o "Check digit". Essa è una forma di controllo usata per il rilevamento dell'errore. Consiste di una sola cifra alfanumerica (ma nel caso delle carte di credito è ovviamente un numero) elaborata da un certo algoritmo partendo dalle altre cifre del codice da verificare. Gli algoritmi che prenderemo in considerazione sono quelli progettati per far fronte agli errori di trascrizione delle persone. Uno dei problemi principali della ricerca e correzione degli errori è la ricerca di algoritmi relativamente semplici (ovvero facilmente implementabili e con un costo computazionale relativamente basso) . In generale gli algoritmi più usati sono quelli basati sulla somma modulo 10 delle cifre che costituiscono il codice. Il loro problema principale è l'incapacità di rilevare errori multipli (come $12 \rightarrow 34$) o errori di trasposizione. Per questo sono stati implementati algoritmi più complessi come ad esempio quelli in cui ogni cifra viene moltiplicata per un determinato peso prima di farne la somma modulo 10 oppure utilizzare altri tipi di congruenze come quella modulo 11 o 97. Per quanto riguarda i codici identificativi delle carte di credito presentiamo l'algoritmo più usato:la formula di Luhn.

5 Formula di Luhn

Consideriamo ora un codice numerico di sedici cifre. La domanda che ci poniamo è la seguente " Può essere il codice identificativo di una determinata carta di credito?". Una possibile risposta alla domanda è data dalla cosiddetta "Formula di Lhun" o "Modulo 10". La formula di Lhun è un algoritmo basato sulle congruenze modulo 10 che ci permette, assegnato un codice numerico, di capire se esso può essere effettivamente il codice identificativo di una carta. Sviluppato intorno al 1954 dal matematico Hans Peter Luhn per conto

dell'IBM, si basa sul calcolo di una particolare cifra che prende il nome di "cifra di Lhun". Se la cifra di Lhun è 0 allora effettivamente si ha un codice identificativo valido, in caso contrario il codice non è valido. Va ricordato che tale algoritmo non va inteso come una funzione hash, ovvero non è progettato per risistere ad attacchi inerenti la sicurezza, ma semplicemente per verificare che non ci siano errori accidentali.

Illustriamo ora come funziona l'algoritmo di Lhun.

1. Partendo da destra e spostandosi verso sinistra si moltiplicano per 2 tutte le cifre poste in posizione pari.
2. In caso una delle moltiplicazioni porti a numeri di due cifre queste vanno sommate per ottenerne una sola.
3. Si sommano le cifre ottenute mediante le moltiplicazioni con quelle dispari. Il numero ottenuto è la "cifra di Lhun".
4. Se il resto della divisione della cifra di Lhun per 10 è nullo allora il codice è valido in caso contrario no.

Detta quindi L la cifra di Lhun abbiamo quindi

$$L =_{mod10} 0 \implies \text{codice valido}$$

$$L \neq_{mod10} 0 \implies \text{codice non valido}$$

Mostriamo ora un esempio di codice valido.

4	0	3	0	2	7	0	9	5	1	9	8	9	6	8	5	$\sum$
8	0	6	0	4	7	0	9	10	1	18	8	18	6	16	5	
8	0	6	0	4	7	0	9	1	1	9	8	9	6	7	5	80

In questo caso $L = 80 \implies 80 \equiv_{10} 0 \implies$ codice valido.

Il seguente esempio è invece il caso di un codice non valido.

4	1	3	2	2	7	0	9	5	1	9	8	9	6	8	7	$\sum$
8	1	6	2	4	7	0	9	10	1	18	8	18	6	16	7	
8	1	6	2	4	7	0	9	1	1	9	8	9	6	7	7	85

$L = 85 \Longrightarrow 85 \neq_{mod10} 0 \Longrightarrow$ codice non valido.

Abbiamo mostrato come dato un codice completo la formula di Luhn ci dice se questo è valido o meno. Possiamo anche affrontare però il problema inverso. Ovvero dato un codice che manca dell'ultima cifra (la cifra di controllo) vogliamo risalire al codice completo. Procediamo nel seguente modo:

1. Indichiamo con X la cifra di controllo mancante
2. Ripetiamo il procedimento di Luhn sul codice "incompleto".
3. Moltiplichiamo la somma ottenuta per 9.
4. L'ultima cifra del risultato è la X cercata.

Applichiamolo all'esempio precedente.

Account number	4	0	3	0	2	7	0	9	5	1	9	8	9	6	8	X	$\sum$
Double every other	8	0	6	0	4	7	0	9	10	1	18	8	18	6	16	X	
Sum of digits	8	0	6	0	4	7	0	9	1	1	9	8	9	6	7	X	75

$\Rightarrow 75 \cdot 9 = 675 \Rightarrow X = 5$

Tra i vantaggi della formula di Luhn vi è sicuramente la sua indubbia semplicità. L'algoritmo è infatti sia molto semplice da capire che da implementare al computer. Esso presenta però anche dei limiti. Può infatti trovare solamente 7 dei 10 tipi di "twin errors". Ad esempio non risce a trovare errori come $22 \rightarrow 55$ oppure $09 \rightarrow 90$.

6 Keylogger e 3-d Secure

Abbiamo visto fin qui i principali codici presenti in una carta di credito
e la loro importanza. In particolare ci siamo soffermati sulla cifra di controllo e sul problema relativo alla sua validità. Ci occupiamo ora di un problema di sicurezza delle carte di credito estremamente recente. Sappiamo che uno degli usi principali della moneta elettronica è quello degli acquisti online. Il rischio che però si corre è

quello di un uso fraudolento da parte di terzi della propria cart. Uno dei problemi sicuramente più grandi è quello dei Keylogger. Un keylogger è uno strumento hardware o software in grado di intercettare tutto ciò che un utente digita sulla tastiera di un computer. I keylogger di tipo hardware vengono collegati al cavo di comunicazione tra la tastiera e il computer o all'interno della tastiera. Essi sono molto efficaci in quanto la loro installazione è molto semplice e il sistema non è in grado di accorgersi della loro presenza. Quando sono installati fra la tastiera e il PC hanno le sembianze di un adattatore o appaiono dei cavi di prolunga. Quando sono nascosti nella tastiera risultano del tutto invisibili. Sono inoltre in grado di leggere anche le password di bootstrap, ovvero quelle password che vengono caricate prima dell'avvio del sistema operativo. I keylogger di tipo software sono invece dei programmi o driver di periferica che rimangono in esecuzione captando i tasti che vengono digitati sulla tastiera del computer. Quest'ultimi sono trasportati e installati nel computer da worm o trojan ricevuti tramite Internet
e hanno in genere lo scopo di intercettare password e numeri di carte di credito e inviarle tramite posta elettronica al creatore degli stessi.La password viene catturata indipendentemente dalla periferica di input (tastiera, mouse, microfono): sia che l'utente la digiti da tastiera, sia che l'abbia salvata in un file di testo prima di collegarsi a Internet, e poi si limiti a inserirla con un copia/incolla, in modo da evitarne la digitazione, sia che la password venga inserita tramite un programma di dettatura vocale. Poiché esistono alcuni tipi di keylogger non intercettabili, per evitare di essere monitorati si può utilizzare la "tastiera sullo schermo", presente in Windows XP/Vista e successivi tra le risorse per l'accesso facilitato, o distribuita da alcuni antivirus come Kaspersky. Per far fronte a questo nuovo tipo di attacchi i circuiti internazionali Visa e MasterCard hanno introdotto dei nuovi sistemi di sicurezza oltre a quelli classici (codice identificativo,codici di sicurezza e codice pin). Il più importante è sicuramente il 3-d Secure (*3 domain Secure*), un protocollo basato sul linguaggio XML sviluppato per aumentare la sicurezza dei pagamenti online con carta di credito, sviluppato inizialmente da Visa e successivamente utilizzato anche da MasterCard ed American Express. Dal 29 gennaio 2008 la registrazione a questo servizio è diventata obbligatoria per poter compiere acquisti online con questi circuiti. Il concetto di base del protocollo è quello di legare il processo di autorizzazione

finanziaria con un'autenticazione online. Tale autenticazione si basa su un modello a tre domini (da qui il nome del sistema di sicurezza):

1. Acquirer Domain (Società che fornisce all'esercente il servizio per l'accettazione dei pagamenti con carta di credito)
2. Issuer Domain (Società che emette la carta di credito)
3. Interoperability Domain (l'infrastrutta fornita per sostenere il protocollo 3-d secure)

Vediamo nei dettagli come avviene l'acquisto mediante il sistema 3-d secure. Per le sigle usate si può fare riferimento al glossario tecnico inserito nella sezione successiva.

1. Il titolare della carta di credito effettua un acquisto su un sito VbV/SCM e inserisce i dati della propria carta, dando inizio alla transazione.
2. Il sito dell'esercente si collega, attraverso la componente Merchant Plug-In (MPI), al Directory Server (di Visa o di MasterCard), inviando un messaggio di tipo VEReq contenente il PAN della carta; il Directory Server verifica se il BIN della carta rientra nella lista dei BIN comunicati dai vari Issuer come aderenti al servizio VbV/SCM e, in tal caso, contatta l'ACS (Access Control Server) dell'Issuer che verifica se la singola carta aderisce al servizio. L'ACS risponde con un messaggio VERes il cui campo PAN Authentication Available indica se un'autenticazione è o non è disponibile per il PAN in questione, assumendo di conseguenza uno di questi valori: Y se l'autenticazione disponibile; N se il titolare non partecipante al servizio o infine U se l'autenticazione non è possibile. Il messaggio VERes è inoltrato al MPI dell'esercente.
3. Se la carta aderisce al servizio, l'MPI invia una richiesta d'autenticazione all'ACS attraverso il messaggio PAReq.
4. l'ACS effettua la fase d'autenticazione secondo le modalità di validazione del pagamento che l'Issuer ha stabilito (tipicamente viene visualizzata sul browser del titolare una pagina per l'inserimento di una password).
5. l'ACS restituisce all'MPI un messaggio PARes i cui campi indicano l'esito dell'autenticazione.

6. Il Merchant Server Plug-in verifica la risposta dell'ACS e decide proseguire o meno con il normale processo autorizzativo.

Caratteristica fondamentale del 3d-secure è che l'esercente che aderisce al servizio viene completamente
esonerato da qualsiasi responsabilità.Nel caso infatti in cui il cliente dovesse disconoscere un'acquisto la responsabilità passa dall'Acquirer all'Issuer. Tale processo viene chiamato "*Liability Shift*". Le regole della Liability shift variano a seconda dei circuiti internazionali a cui si aderisce.

7 Glossario tecnico

MPI (Merchant Plug-in): Componente del protocollo 3d Secure che consente al merchant di collegarsi con i circuiti e con l'ACS per effetturare la fase di autenticazione.

ACS (Access Control Server):Componente del protocollo 3D Secure gestita dall'Issuer che verifica se una carta aderisce al protocollo e ne effettua l'autenticazione.

VEReq (Verify Enrolment Request):Messaggio del protocollo 3D Secure inviato dall'MPI alla Directory Server per verificare se la carta partecipa al VbV o al SecureCode.

VERes (Verify Enrolment Response):Messaggio del protocollo 3D Secure inviato in risposta al messaggio VEReq. Indica se la carta partecipa al VbV o al SecureCode.

PAReq (Payer Authentication Request):Messaggio del protocollo 3D Secure, inviato dall'MPI per richiedere l'autenticazione del titolare.

PARes (Payer Authentication Response:)Messaggio del protocollo 3D Secure, inviato come risposta al messaggio PAReq. Contiene l'esito della fase d'autenticazione del titolare.

References

[1] Wikipedia,l'enciclopedia libera.

[2] Carta SI. Allegato tecnico e-commerce.

[3] S. Leonessi – C. Toffalori, Numeri e crittografia, Springer 2006