



LA MONETA ELETTRONICA

A cura di: Di Matteo Francesco-Albano Giuseppe-Ambrosino Gianluca

INTRODUZIONE

Buongiorno, ha da cambiarmi la 50?

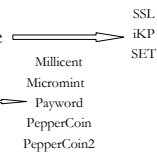
Quante volte abbiamo ascoltato questa frase, chissà se riusciremo ad eliminarla in futuro.

Uno degli obiettivi della moneta elettronica è proprio questo.

INTRODUZIONE

Nel nostro lavoro affronteremo...

- Problema generale della sicurezza delle reti
- Vari pagamenti elettronici
- Protocolli per le transazioni sicure
- Sistemi Digital Cash
- Protocolli di pagamento



SICUREZZA DELLE RETI

Adottare adeguate misure per proteggere i dati da intrusioni o da un loro utilizzo diverso da quello previsto dai legittimi possessori

Tecnica base: Crittografia

- Simmetrica
- Asimmetrica

SICUREZZA DELLE RETI

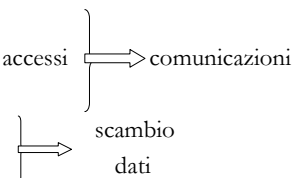
Funzionalità necessarie per garantire che gli scambi di informazioni tra il sistema e la rete siano protetti:

- Autenticazione
- Controllo degli accessi
- Riservatezza
- Integrità
- Non ripudio

SICUREZZA DELLE RETI

Funzionalità necessarie per garantire che gli scambi di informazioni tra il sistema e la rete siano protetti:

- Autenticazione
- Controllo degli accessi
- Riservatezza
- Integrità
- Non ripudio



SICUREZZA DELLE RETI

Ruolo importante lo giocano i:

CERTIFICATI DIGITALI

≈

CARTA D' IDENTITA'

7

SICUREZZA DELLE RETI

PROTOCOLLO SSL

Il protocollo SSL provvede alla sicurezza del collegamento garantendo tre funzionalità fondamentali:

1. Privatezza del collegamento
2. Autenticazione
3. Affidabilità

8

SICUREZZA DELLE RETI

PROTOCOLLO SSL

H.T.T.P
SSL HANDSHAKE
SSL RECORD
T.C.P.
I.P.

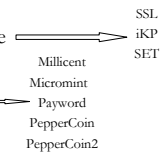
SSL è un protocollo a due strati, SSL Record a livello inferiore ed SSL Handshake a livello superiore, che si interfaccia con una applicazione ad esempio HTTP

9

INDICE

Nel nostro lavoro affronteremo...

- Problema generale della sicurezza delle reti
- Vari pagamenti elettronici
- Protocolli per le transazioni sicure
- Sistemi Digital Cash
- Protocolli di pagamento



10

PAGAMENTI ELETTRONICI

I sistemi di pagamento elettronici possono essere classificati in:

- Carta di credito
- Assegni elettronici
- Borsellino elettronico
- E-cash

11

PAGAMENTI ELETTRONICI

Pagamenti On-line v.s. Off-line

On-line: coinvolgendo un server di autenticazione e autorizzazione.

Off-line: non si ricorre ad una terza parte durante la transazione tra compratore e venditore.

12

PAGAMENTI ELETTRONICI

Pagamenti On-line v.s. Off-line

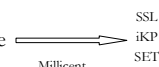
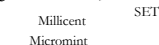
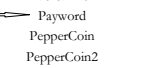
Problema in Off-line: come far sì che il compratore non spenda più denaro di quello che attualmente possiede ?

...Hardware affidabile...Smartcard...

13

INDICE

Nel nostro lavoro affronteremo...

- Problema generale della sicurezza delle reti
- Vari pagamenti elettronici
- Protocolli per le transazioni sicure 
- Sistemi Digital Cash 
- Protocolli di pagamento 

14

Internet Keyed Payment Protocol

Il protocollo iKP sviluppato dalla IBM, è un prototipo di sistema di pagamento su Internet basato su carta di credito.

Originariamente pensato come contributo alla standardizzazione

e poi...

15

Internet Keyed Payment Protocol

progettato per:

- Ottenere un alto livello di integrità per tutte le parti coinvolte, tenendo conto delle differenze di rischio e di esigenze tra una parte e l'altra.
- Fornire riservatezza nelle transazioni economiche.
- Lavorare con il minimo impatto sui sistemi finanziari esistenti.

ma...

16

Internet Keyed Payment Protocol

...Non consente alcuna trattativa su modalità di pagamento, prezzo ecc.: contiene una semplice procedura di contratto ("offerta/ordine").

- Non fornisce la non tracciabilità dei pagamenti (ma protegge dal venditore i dati del compratore).
- Non fornisce mezzi per una distribuzione sicura di informazioni: fornisce ricevute di pagamento ma non le protegge.

17

Internet Keyed Payment Protocol

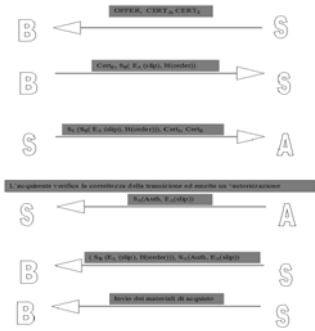
Esistono tre varianti del protocollo iKP, identificate dal valore dell'indice *i* presente nel nome:

- 1KP solo l'acquirente può firmare i messaggi (cioè solo l'acquirente possiede una coppia di chiavi pubblica e privata).
- 2KP anche il venditore può firmare (esistono due proprietari di coppie di chiavi).
- 3KP anche il compratore può firmare (esistono tre proprietari di coppie di chiavi).

18

Internet Keyed Payment Protocol

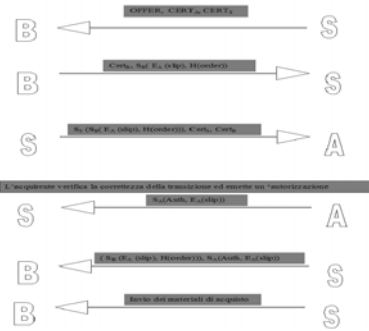
1kp



19

Internet Keyed Payment Protocol

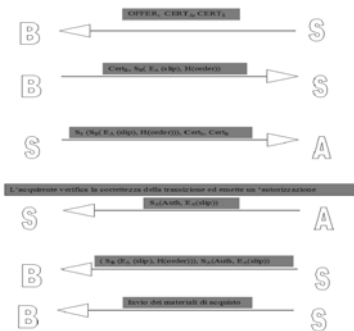
2kp



20

Internet Keyed Payment Protocol

3kp



21

Internet Keyed Payment Protocol

2KP vs. 3KP

- In 3KP il compratore è responsabile solo per gli ordini di pagamento da lui firmati.
- In 2KP con passphrase segreta nello slip (2KP+), l'acquirente può facilmente falsificare ordini di pagamento, e non esiste alcun modo di provarlo. Esiste sicurezza verso esterni, anche per passphrase relativamente corte (come PIN, per esempio), dal momento che non sono possibili attacchi tipo del dizionario.
- In 2KP senza segreto (2KP-) chiunque conosca i dati del pagamento può effettuare pagamenti falsi.

22

Secure Electronic Transaction

- VISA e Mastercard hanno sviluppato congiuntamente il protocollo SET come metodo per il pagamento sicuro su reti aperte.
- Obiettivi che il SET si prefigge...

23

Secure Electronic Transaction

...sulla sicurezza

- Garantire la riservatezza dell'informazione.
- Assicurare l'integrità dei pagamenti.
- Autenticare compratore, venditore e acquirente.
- Definire algoritmi e protocolli necessari per tali servizi.

24

Secure Electronic Transaction

...sulla interoperabilità

- Definire informazioni dettagliate per assicurare che applicazioni sviluppate da un venditore lavorino con applicazioni sviluppate da altri venditori.
- Creare e supportare uno standard aperto per pagamento con carte di credito.
- Sfruttare gli standard esistenti, quando possibile.
- Consentire l'implementazione su ogni combinazione di piattaforme hardware e software come Power PC, Intel, Sparc, UNIX, MS-DOS, OS/2, Windows, Macintosh.

25

Secure Electronic Transaction

...sulla accettazione

- Ottenere un'accettazione globale, tramite una facile implementazione e un impatto minimo su venditore e compratore.
- Sfruttare le applicazioni per clienti già esistenti.
- Minimizzare lo scambio di relazioni tra acquirente e venditore, e tra compratore e fornitore.
- Fornire un protocollo efficiente dal punto di vista delle istituzioni finanziarie.

26

Secure Electronic Transaction

Nel SET tre novità:

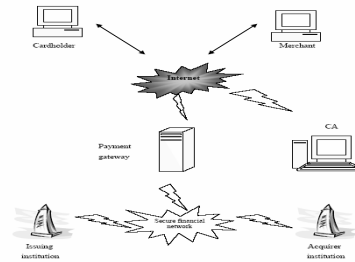
- la *certification authority*, che certifica i partecipanti;
- il *payment gateway*, che fa da filtro tra Internet e la rete bancaria;
- la *dual signature*, la doppia firma.

Sei partecipanti:

- il *cardholder* (il possessore della carta di credito), la cui carta è conforme alle specifiche SET è stata emessa da una istituzione preposta, tipicamente banche affiliate con Visa e MasterCard;
- il *server del Commerciante*;
- il *payment gateway*; (*Gateway di pagamento*);
- l'*issuing institution* (l'istituzione che emette la carta di credito);
- la *Certification Authority (CA)*;
- l'*Acquiring Institution*, che è la banca del commerciante.

27

Secure Electronic Transaction



28

Secure Electronic Transaction

Servizi di sicurezza del SET

Le transazioni SET forniscono i seguenti servizi:

- Registrazione dei cardholder (possessore della carta di credito) e dei merchant (commercianti) con la CA;
- Consegna di certificati ai cardholders ed ai merchant;
- Autenticazione, riservatezza ed integrità delle transazioni di acquisto; autorizzazione di pagamento.

SET Usa tecniche di crittografia a chiave pubblica per garantire simultaneamente:

- Riservatezza degli scambi;
- Integrità dei dati scambiati tra il cliente, il merchant e l'acquiring bank;
- Identificazione e Autenticazione dei partecipanti;
- Una condizione necessaria ma non sufficiente per il non ripudio della transazione è che il possessore della carta sia certificato.

29

Secure Electronic Transaction

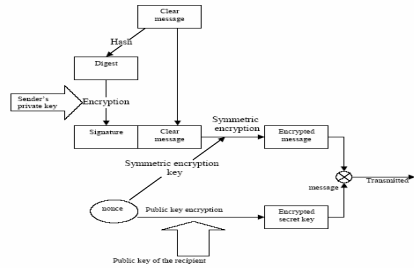
Algoritmi usati nel SET

ALGORITMO	SERVIZI
DES	Riservatezza
RSA	Autenticazione, identificazione, integrità
SHA1	Hashing
HMAC-SHA1	Keyed hashing

30

Secure Electronic Transaction

Trattamento di un messaggio nel SET.



31

Secure Electronic Transaction

Cifratura da parte di A

Decifratura da parte di B

- 1) $H=h(M)$;
- 2) $F=\text{firma}(H,d_A)$;
- 3) $M'=\text{cifra}_r(M,F,C_A)$;
- 4) $K=\text{cifra}_{e_B}(r)$;
- 5) spedire a Bob M',K

- 1) $r = \text{decifra}_{d_B}(K)$;
- 2) $(M,F,C_A) = \text{decifra}_r(M')$;
- 3) $H = \text{decifra}_e(F)$;
- 4) $H=h(M)$;
- 5) $H=H?$

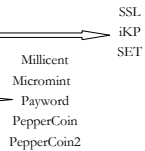
M = messaggio da cifrare
 h = funzione hash
 d_A = chiave privata di signature di A
 e_A = chiave pubblica di signature di A
 d_B = chiave privata di key-exchange di B
 e_B = chiave pubblica di key-exchange di B
 r = chiave simmetrica casuale
 C_A = certificato di signature di A
 cifra_r = algoritmo di cifratura con chiave k
 decifra_r = algoritmo di decifratura con chiave k
 firma = algoritmo di firma

32

INDICE

Nel nostro lavoro affronteremo...

- Problema generale della sicurezza delle reti
- Vari pagamenti elettronici
- Protocolli per le transazioni sicure
- Sistemi Digital Cash
- Protocolli di pagamento



33

SISTEMI DIGITAL CASH

Proprietà per i sistemi Digital Cash:

- Sicurezza
- Anonimato
- Scalabilità
- Accettabilità
- Trasferibilità
- Indipendenza dell' hardware
- Diverse tipologie di pagamento

34

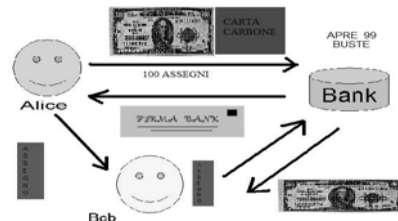
SISTEMI DIGITAL CASH

Facciamo una panoramica sui protocolli...

35

SISTEMI DIGITAL CASH

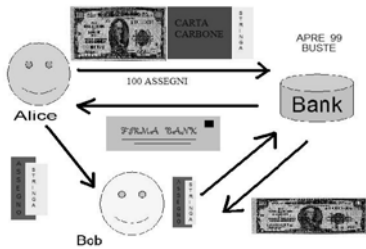
PROTOCOLLO DIGITAL CASH 1



36

SISTEMI DIGITAL CASH

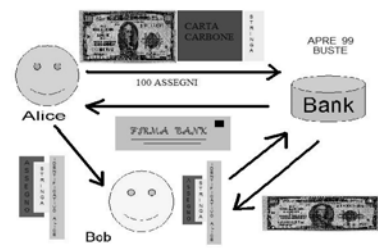
PROTOCOLLO DIGITAL CASH 2



37

SISTEMI DIGITAL CASH

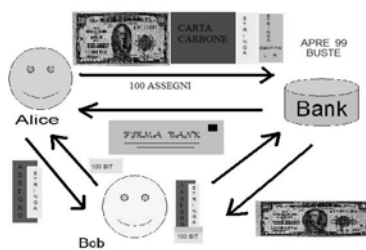
PROTOCOLLO DIGITAL CASH 3



38

SISTEMI DIGITAL CASH

PROTOCOLLO DIGITAL CASH 4



39

SISTEMI DIGITAL CASH

ATTACCO: CRIMINE PERFETTO

- A rapisce un bambino;
 - A prepara 10000 assegni anonimi di qualsiasi cifra;
 - A nasconde questi assegni con il protocollo di firma digitale e manda tutto alle autorità con le seguenti richieste che se non esaudite comporterebbero l'uccisione del bambino:
 - una banca deve firmare tutti assegni;
 - pubblicare i risultati su di un giornale;
 - le autorità accettano;
 - A verifica l'avvenuta pubblicazione, scopre gli assegni e li spende;
 - A rilascia il bambino.
- Lo schema del crimine perfetto rappresenta l'unico modo per poter attaccare con successo il protocollo 4.

40

SISTEMI DIGITAL CASH

ECASH

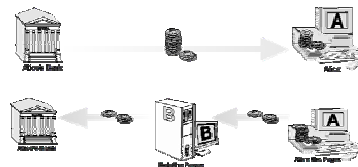
- Ecash è un sistema di pagamenti sicuri per Internet elaborato da Digicash società fondata dal Dott. David Chaum.
- Per poter utilizzare Ecash è necessario aprire un conto con una delle banche partecipanti. Sarà poi possibile memorizzare sul proprio computer monete elettroniche; tali monete, al momento di un acquisto, verranno trasferite al venditore sfruttando tecniche di crittografia a chiave pubblica e di firma digitale.

41

SISTEMI DIGITAL CASH

ECASH

- Operare con Ecash è piuttosto semplice: è sufficiente procurarsi il software Ecash client e aprire un conto con una delle banche partecipanti.



42

SISTEMI DIGITAL CASH

ECASH

- Per garantire sicurezza e riservatezza Ecash sfrutta tecniche di firma digitale a chiave pubblica. I prelievi di ecash dal conto di ogni utente sono inoltre protetti da una password nota esclusivamente all'utente stesso.



43

INDICE

Nel nostro lavoro affronteremo...

- Problema generale della sicurezza delle reti
 - Vari pagamenti elettronici
 - Protocolli per le transazioni sicure
 - Sistemi Digital Cash
 - Protocolli di pagamento
- SSL
iKP
SET
Millicent
Micromint
Payword
PepperCoin
PepperCoin2

44

MILLICENT

Millicent è un protocollo progettato per l'implementazione della moneta elettronica sul server del commerciante senza:

- comunicazioni aggiuntive
- onerose operazioni di crittografia
- processing fuori linea

Il protocollo si basa su scrips e su brokers...

45

MILLICENT

- Quando un cliente effettua un acquisto con lo scrip, il costo dei beni è scalato dal bilancio dello scrip stesso.
- Il cliente stabilisce un account con il broker mentre quest'ultimo lo stabilisce con il commerciante.
- L'account tra cliente e commerciante può essere visto come suddiviso in due parti:
 - cliente -> broker;
 - broker -> commerciante.
- Un cliente ha un solo account con un broker; ciascun venditore ha un ridotto numero di account con i broker. Il cliente gestisce il bilancio dell'account senza rischi per il venditore, il quale è tutelato da modifiche del bilancio da una firma digitale. Allora il commerciante al più verifica la correttezza del valore dello scrip senza dover memorizzare i movimenti effettuati dal cliente.

46

MILLICENT

Scrip: è la base di una famiglia di protocolli millicent.

Validazione e scadenza sono ottenute in due passi :

- il certificato è ricalcolato e controllato con il certificato inviato. Se lo scrip è stato falsificato, allora non c'è match;
- c'è un unico ID incluso nel corpo dello scrip ed il commerciante può verificare se la moneta è stata già spesa.

E il **broker**...

...si pone tra il cliente ed il venditore e manipola tutte le transazioni in moneta reale.

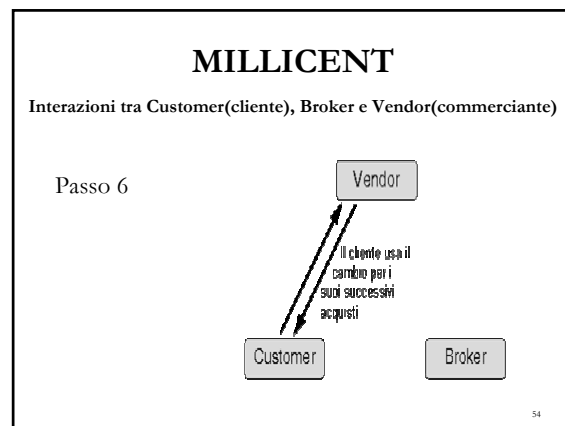
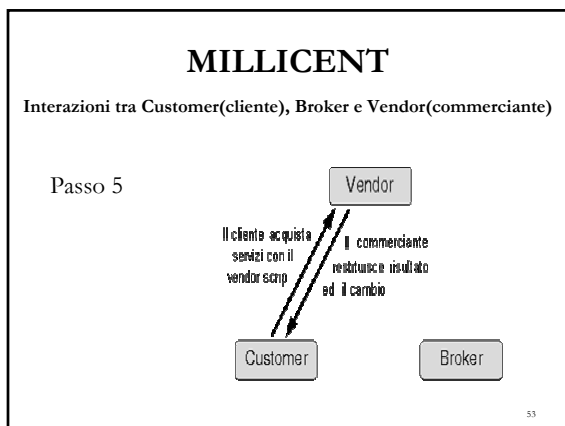
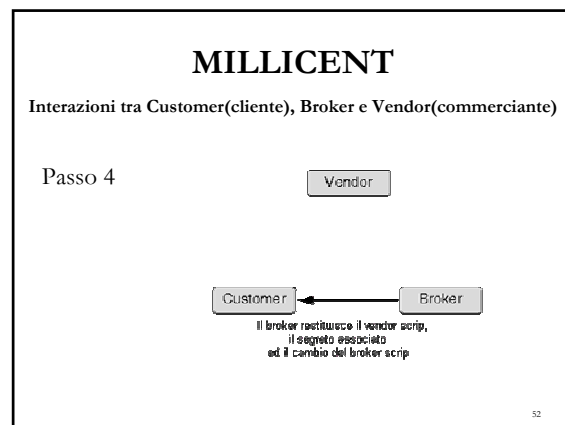
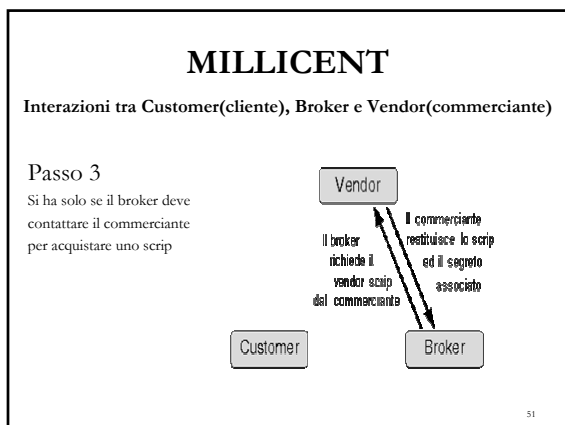
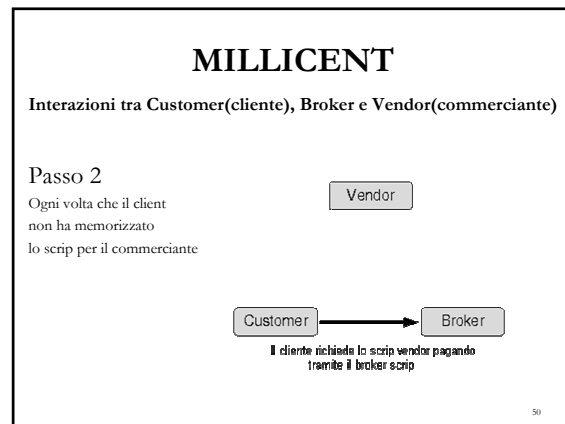
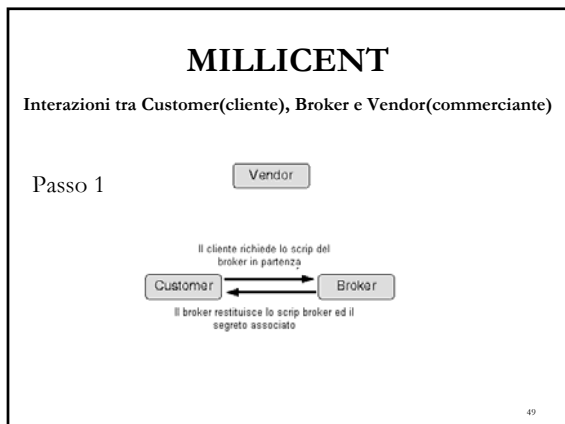
47

MILLICENT

I tre protocolli più importanti della famiglia Millicent basati su scrip:

- Il più semplice ed efficiente, ma meno sicuro:
"scrip in the clear"
- Buona privacy, ma è più costoso:
"private and secure"
- Altrettanto sicuro, ma più efficiente:
"secure without encryption"

48



MICROMINT

- Le monete sono prodotte da un broker, che le distribuisce agli utenti.
- Gli utenti girano queste monete ai venditori come pagamento.
- I venditori restituiscono le monete al broker che ne rimborsa l'ammontare attraverso altri mezzi.
- Una moneta è una stringa di bit la cui validità può essere facilmente constatata da ognuno, ma che è difficile da produrre.

Generare più monete risulta più conveniente di generarne poche.

55

MICROMINT

- Le monete di MicroMint sono rappresentate da collisioni di funzioni hash.



one-way h che trasformano stringhe x di m bit in stringhe y di n bit

- La sicurezza si raggiunge scegliendo le collisioni a k -vie.
- Una collisione a k -vie è un'insieme di k valori distinti x_1, \dots, x_k che hanno lo stesso valore hash y .

56

MICROMINT

- Il broker inizia la distribuzione delle monete ai suoi clienti verso la fine di ogni mese.
Queste monete verranno poi utilizzate nel mese successivo e soltanto all'inizio del mese rende pubblico il criterio per ritenerle valide.
- I clienti che comprano monete caricano questo acquisto sulla propria carta di credito.
- Il broker da parte sua tiene traccia delle monete distribuite ai singoli utenti.

57

MICROMINT

- Ogni volta che un cliente deve pagare un acquisto ad un venditore gli spedisce la serie $x=x_1, x_2, \dots, x_k$ che forma la moneta.
- Quest'ultimo controlla che sia una moneta valida calcolando l'hash su ogni valore della serie e verificando che è uguale per tutti (collisione a k -vie).
- Il venditore, ogni giorno, restituisce al broker le monete che ha accumulato.
- Il broker controlla le varie monete tentando di individuare eventuali monete che sono state già riscattate.
 - ✓ Per monete valide paga al venditore la somma stabilita.
 - ✓ Per quelle che gli sono state inviate più volte sceglie di pagare uno solo dei venditori, finendo penalizzando gli altri.

58

MICROMINT

ATTACCHI

Gli attacchi possibili ad uno schema Micromint si dividono in larga e piccola scala.

Cioè se portano a consistenti guadagni o a piccoli guadagni per eventuali contraffattori

Tre tipi di attacchi...

59

MICROMINT

Contraffazione

Contrastata invalidando le monete a fine mese e ritardando il criterio di validità.

Furto di monete

Avviene nella fase di distribuzione e un possibile contrasto è cifrare questa fase.

Riutilizzo di monete

Micromint non garantisce l'anonimato e quindi il broker può individuare i venditori che gli hanno fornito le diverse copie.

60

PAYWORD

- PayWord è una catena di gettoni che vengono ceduti uno alla volta dal cliente, che li genera, al commerciante.
- Il commerciante provvede in seguito a riscuoterli presso la banca del cliente.
- Di questi, solo il primo viene autenticato con firma digitale.

61

PAYWORD

ASPETTO CRITTOGRAFICO...

- Verrà utilizzata la crittografia a chiave pubblica (esempio RSA)

Con sei chiavi:

- PKB = Chiave pubblica Broker
- SKB = Chiave privata Broker
- PKU = Chiave pubblica Utente
- SKU = Chiave privata Utente
- PKV = Chiave pubblica Vendor(Commerciante)
- SKV = Chiave privata Vendor(Commerciante)

62

PAYWORD

Protocollo...

Possiamo dividerlo in tre parti:

UTENTE – BROKER
UTENTE – VENDITORE
VENDITORE - BROKER

63

PAYWORD

Protocollo...

UTENTE – BROKER

Rapporti e certificati

- L'utente U inizia un rapporto con il broker B aprendo presso di lui un conto e richiedendogli un certificato payword.
- U invia a B su un canale sicuro: il suo numero di carta di credito, la sua chiave pubblica PKU ed il suo indirizzo di consegna AU.
- Il certificato dell'utente ha una data di scadenza E.

64

PAYWORD

Protocollo...

UTENTE – VENDITORE

Ordini

- Quando un utente U sta per contattare un nuovo venditore V calcola una nuova serie di payword w_1, \dots, w_n con radice w_0 .
- Il valore n è scelto dall'utente a proprio piacimento.
- Calcola il suo ordine per quella serie.
- L'ordine autorizza B a pagare V per ognuna delle payword.

Pagamenti

- L'utente ed il venditore devono essere d'accordo sull'ammontare del pagamento.
- Il pagamento è costituito da una stringa lunga solo 20 o 30 bit.
- Il pagamento non è firmato da U dal momento che è autenticato usando l'ordine.
- L'utente spende le sue payword in ordine sequenziale w_1 poi w_2 e così via.

65

PAYWORD

Protocollo...

VENDITORE - BROKER

Rapporti e retribuzioni

Un venditore V deve:

- necessariamente conoscere PKB per poter autenticare i certificati firmati da B.
- stabilire con B le modalità con cui riscuotere i pagamenti che ha ricevuto.
- Al termine di ogni giornata invia a B, per ogni utente che lo ha pagato quel giorno, un messaggio contenente l'ordine CU insieme all'ultimo pagamento da questi effettuato.

Un Broker B deve:

- verificare ogni ordine utilizzando PKU.
- valutare il pagamento.

66

PEPPERCOIN

Peppercoin è una società di pagamento

Protocollo su cui si fonda Peppercoin è :

Lo Schema MR02

Miglioramento di MRO1 dove il problema principale era la possibilità di pagamenti eccessivi sostenuti dall'utente.

67

MR02

Il piccolo rischio di un pagamento eccessivo è passato dall'utente alla banca.

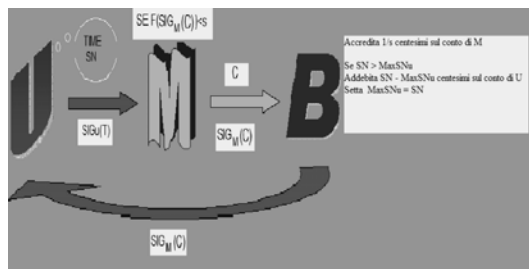
Questo è preferibile per due motivi:

1. pagamenti eccessivi accadono molto raramente, e per un ammontare moderato, e le banche sono abituate a gestire rischi maggiori;
2. il rischio relativo a lungo andare tende a diminuire, e così è meno probabile per la banca, dato che ha un'esperienza ben più grande del singolo utente.

68

MR02

SCHEMA BASE



69

MR02

Variante teorica:

- Risulta cruciale che $F(\text{SIG}_M(C))$ sia un numero casuale, sufficientemente grande in modo da garantire la sicurezza dall'utente malizioso. Questa condizione di sicurezza dipende dallo schema di firma e dalla definizione di F , schemi di firma consigliati:
 - ✓ Oracolo Casuale
 - ✓ RSA
- Lo stesso punto cruciale però può essere risolto per il commerciante utilizzando una funzione casuale verificabile (VRF) piuttosto che uno schema di firma digitale ordinario.

70

MR02

Variante pratica

Si può operare su vari parametri:

Tempo:

Lo schema base permette ad un commerciante di depositare un check pagabile in qualsiasi istante.

La banca può rifiutare di accreditare il conto del commerciante durante la fase di deposito a meno che non presenti un check pagabile che ha un tempo sufficientemente corretto.

Questo da uno stimolo in più al commerciante per verificare la correttezza del tempo del check che egli riceve.

Invece se il tempo è errato, egli può rifiutare di fornire la "merce" richiesta. Il temporaneo deposito assicura che all'utente non venga addebitato "troppo tardi", altrimenti spenderebbe dei soldi che in realtà non possiede.

e...

71

MR02

...Funzioni F e G:

- Le funzioni F e G possono non essere fissate, ma variare.
- Per ogni istanza, un check o una transazione possono specificare quale F o G debba essere usata con loro.
- Le condizioni di pagabilità del check $F(\text{SIG}_M(C)) < s$, potrebbe essere rimpiazzato da $F(\text{SIG}_M(G(C))) < s$, dove G è una data funzione/ algoritmo.
- Piuttosto che firmare C stesso, il commerciante può firmare una quantità dipendente da C , denotata da $G(C)$.
- Per minimizzare il numero di firme del commerciante, piuttosto che usare $F(\text{SIG}_M(G(C)))$, si può usare $F(\text{SIG}_M(G(V_i)))$, dove $\{V_i\}$ è una sequenza di valori associati ad una sequenza di istanti.
- Un check C relativo ad una transazione T in un certo giorno i può essere pagabile se $F(\text{SIG}_M(V_i)) < s$.

72

PEPPERCOIN V.S. PEPPERCOIN 2

PROTOCOLLI	PEPPERCOIN 1.0	PEPPERCOIN 2.0
INTERVALLO DELLE TRANSAZIONI	MICROPAGAMENTI (meno di €0,00)	PICCOLI PAGAMENTI (meno di €20,00)
MERCATO	ONLINE	ONLINE, PUNTI VENDITA FISICI E.CC.
PRATICA RICHIESTA AL CONSUMATORE	DOWNLOAD E INSTALLAZIONE DEL "PORTAFOGLIO"	NORMALE CARRELLO PER GLI ACQUISTI, INTERFACCIA STANDARD PER LE TRANSAZIONI CON CARD
VINCOLI PER IL CONSUMATORE	RICHIESTA DI PRE-REGISTRAZIONE, TERMINI E CONDIZIONI SUL CREDITO "DETTATE" DA PEPPERCOIN	NESSUN SET-UP PER LA REGISTRAZIONE, NESSUN DIRITTO OLTRE QUELLI COMUNI PER IL COMMERCIANTE
SUPPORTO PER IL CONSUMATORE	I COMMERCIANTI SONO RESPONSABILI DI RISOLVERE LE DISPUTE CON I CONSUMATORI	PEPPERCOIN PREVEDE SERVIZI AUTOMATICI PERSONALIZZATI PER LE DISPUTE
MODELLI DI COMMERCIO	PAGARE PER SCARICARE	PAGARE PER USARE, SOTTOSCRIZIONI E ACCESSO PREPAGATO
PAGAMENTO	I COMMERCIANTI SONO PAGATI BASANDOSI SU COMPLESSI ALGORITMI STATISTICI A CAMPIONE	I COMMERCIANTI SONO PAGATI BASANDOSI SU CIO' CHE VERAMENTE HANNO VENDUTO

73

LINK DI RIFERIMENTO

www.cybercash.com/

(Illustra i servizi di pagamento su internet)

www.glenbrook.com/pdf/

(Contiene informazioni sul protocollo Peppercoin 2.0)

<http://www.lcs.mit.edu/publications/publications.php>

(Contiene informazioni sullo schema MR02)

www.theory.lcs.mit.edu/~cis/pubs/rivest/

(Illustra i protocolli PayWord e Micromint)

www.theory.lcs.mit.edu/~rivest/

(Contiene informazioni sul protocollo Peppercoin)

www.w3.org/Conferences/WWW4/Papers/246/#SECTION500

(Contiene informazioni sul protocollo Millicent)

74