Vendere online

Andrea Marin

Università Ca' Foscari Venezia
SVILUPPO INTERCULTURALE DEI SISTEMI TURISTICI
SISTEMI INFORMATIVI PER IL TURISMO

a.a. 2013/2014

Section 1

Introduzione

Vendere online

- Parliamo di acquisti online quando a seguito della consultazione di una pagina o portale web avviene effettivamente un acquisto con una transazione economica
- Il trading online in Italia è meno diffuso che in altri Paesi
  - Trend di continua espansione
- Problema della percezione dei rischi connessi al pagamento
- Problema della percezione dei rischi di truffa sulla merce
- Opportunità di vendere ad una vasta platea pur disponendo di ridotte risorse finanziarie

Quando conviene?

- Il trading online deve essere integrato all'interno di una strategia d'azienda
- L'acquisto deve essere semplice e l'utente deve capire bene...
  - Costi
  - Cosa acquista
  - Convenienza
- Attenzione: perdere la reputazione sul web è fin troppo facile!

Sicurezza dei pagamenti online

- Il trading online ammette diverse forme di pagamento...
  - Contrassegno (per merce consegnata)
  - Carta di credito
  - Conto online (e.g. Paypal)
  - Bonifico bancario
- Carte di credito e conti online consentono una gestione degli ordini completamente automatica e praticamente istantanea
  - Quali sono i rischi connessi con questi pagamenti?

Cosa accade nella rete

- Nell'affrontare il problema della sicurezza online dobbiamo fare alcune assunzioni su cosa può fare un malintenzionato sul web
- In realtà questi ha grandi opportunità:
  - Può leggere qualunque informazione trasmessa
  - Può modificare le informazioni trasmesse
  - Può spacciarsi per un altro utente
  - Può impedire che delle informazioni arrivino a destinazione
  - Può replicare dei pacchetti di informazioni inviate da altri
- C'è speranza di sicurezza?
  - Sì

Crittografia

- La crittografia è una disciplina che, dato un messaggio in chiaro M lo rende incomprensibile se non al destinatario
- Formalmente, siano:
  - M il messaggio in chiaro
  - M' il messaggio crittografato
  - f la funzione associata all'algoritmo di trasformazione
- Quindi abbiamo:

$$M' = f(M)$$

- Per decifrare un messaggio usiamo una funzione g, quindi:

$$M = g(M')$$

Uso delle chiavi

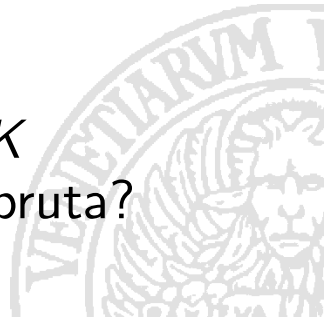
- Nella moderna crittografia la segretezza non risiede nel funzionamento delle funzioni f e g
  - Gli algoritmi di crittografia sono pubblici
- Per garantire la segretezza delle trasmissioni si usano delle chiavi
- La funzione f quindi prende una chiave K e un messaggio M e lo cifra in M'
  - In generale M' dipende sia da M che da K
- Anche la funzione g, per decifrare il messaggio, necessita di una chiave

Chiavi simmetriche

- Un sistema di crittografia si dice a chiave simmetrica se il mittente (usa funzione f) ed il destinatario (usa la funzione g) devono conoscere la stessa chiave per comunicare, cioè:

$$M' = f_K(M) \text{ e } M = g_K(M')$$

  - $f_K(M)$ denota la funzione che cifra M usando la chiave K
  - $g_K(M')$ denota la funzione che decifra M' usando la chiave K
- Problema: come scambiarsi le chiavi K da usare in una comunicazione?
  - Tutta la sicurezza risiede nella segretezza della chiave K
  - Potrebbe essere scoperta mediante un attacco fi forza bruta?
    - forza bruta: provare tutte le possibili chiavi



Chiavi asimmetriche

- Gli attori A e B hanno due chiavi ciascuno K_A^+, K_A^-, K_B^+ e K_B^-
  - K_*^+ è chiamata chiave pubblica che l'attore rivela a tutti
  - K_*^- è chiamata chiave privata che l'attore tiene segreta
- I messaggi cifrati con la chiave pubblica (es. K_A^+) vengono decifrati con quella privata (K_A^-) e viceversa
- Quindi abbiamo:

$$M' = f_{K_A^+}(M) \text{ e } M = g_{K_A^-}(M')$$

$$M' = f_{K_A^-}(M) \text{ e } M = g_{K_A^+}(M')$$

- Dalla chiave pubblica non si riesce a dedurre la chiave privata associata

Garantire la segretezza

- Scenario:
  - A vuole mandare un messaggio a B senza che sia comprensibile da possibili malintenzionati
    - Esempio: A vuole inviare a B un numero di carta di credito M
  - A usa la chiave pubblica di B per cifrare il messaggio:
    - $M' = f_{K_B^+}(M)$
  - Quando B riceve il messaggio usa la propria chiave privata per decifrarlo
    - $M = g_{K_B^-}(M)$

Garantire l'autenticità

- Autenticità: sono certo del mittente di un messaggio
- A vuole mandare a B un messaggio pubblicamente leggibile, ma vuole garantire che l'autore è se stesso
- A cifra il messaggio M con la propria chiave privata K_A^-
  - $M' = f_{K_A^-}(M)$
- B decifra il messaggio con la chiave pubblica di A
  - $M = g_{K_A^+}(M')$
- Come garantire autenticità e segretezza?

Implementazioni

- Esempi di algoritmi a chiave simmetrica sono: IDEA, DES, AES, ...
  - Tipicamente sono molto veloci
- Esempi di algoritmi a chiave pubblica sono: RSA, Crittografia a curve ellittiche, ...
  - Tipicamente molto più lenti di quelli a chiave simmetrica

Hashing

- A differenza dei normali algoritmi di crittografia l'hashing è non invertibile e non usa chiavi
- Sia M il messaggio e h la funzione associata all'algoritmo di hashing:

$$M' = h(M)$$

- Non cè modo di risalire a M quando è noto M'

Firma digitale

- Scenario: A vuole mandare un messaggio a B in chiaro ma garantendo la propria identità
- A potrebbe cifrare completamente il proprio messaggio con K_A^-, ma...
  - Potrebbe richiedere molto tempo
  - Comunque il messaggio non sarebbe immediatamente comprensibile
- A calcola l'hash del messaggio $M' = h(M)$
- A cifra M' con la propria chiave privata: $M'' = f_{K_A^-}(M')$
  - M'' prende il nome di firma digitale del messaggi
- A invia un messaggio formato dalla concatenazione di M e M''

Ricezione di un messaggio firmato

- B riceve un messaggio in cui l'autore si dichiara essere A
- Il messaggio è composto da una parte in chiaro M e da una firma M''
- B recupera la chiave pubblica di A e decifra M'' ottenendo M':

$$M' = g_{K_A^+}(M'')$$

- B calcola l'hash del messaggio M ottenendo M''':

$$M''' = h(M)$$

- Se $M''' = M'$ allora B è sicuro che:
  - Il mittente è veramente A
  - Il messaggio M ricevuto non è stato alterato prima della ricezione

Certificato

- Un problema degli algoritmi a chiave asimmetrica è come stabilire se una chiave pubblica appartiene veramente ad una persona
- Ad esempio:
  - Voglio inviare il mio numero di carta di credito a PayPal
  - Come faccio a conoscere la chiave pubblica di PayPal?
    - Un truffatore potrebbe spacciarsi per PayPal nel web
- I certificati elettronici risolvono questo problema

Enti di certificazione

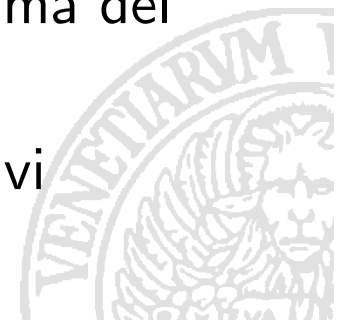
- Gli enti di certificazione sono delle organizzazione governative o non che certificano che un attore è associato ad una certa chiave pubblica
- Questo consente agli utenti di inviare a quell'attore messaggi segreti e di ricevere da quell'attore messaggi autentici
- La certificazione avviene per via elettronica
- Un'azienda seria si dota di certificato elettronico

Struttura di un certificato elettronico

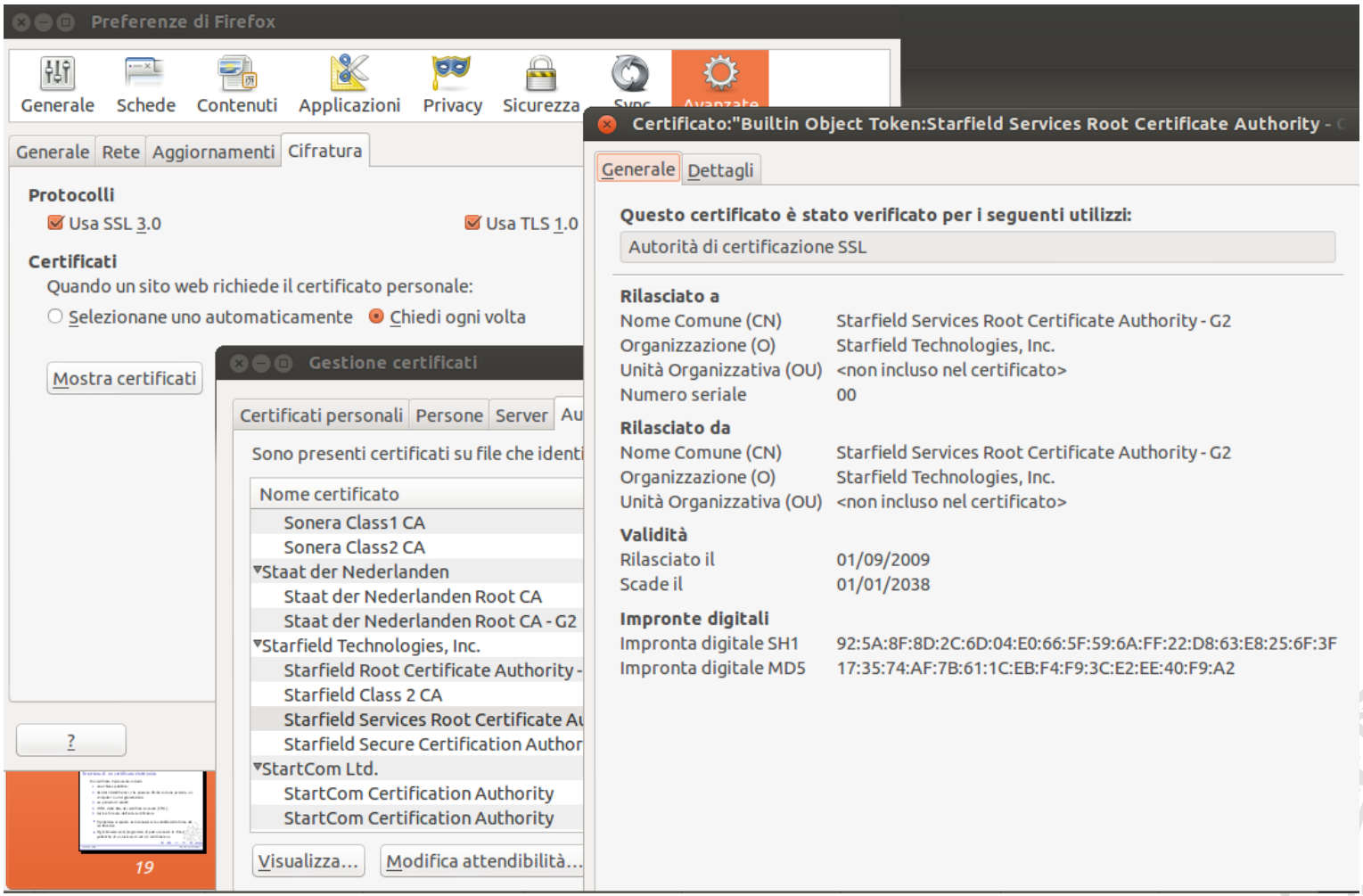
Un certificato tipicamente include:

1. una chiave pubblica;
2. dei dati identificativi, che possono riferirsi ad una persona, un computer o un'organizzazione;
3. un periodo di validit;
4. l'URL della lista dei certificati revocati (CRL);
5. tutto è firmato dall'ente certificatore

- Il problema si sposta nel riconoscere la validità della firma del certificatore
- Ogni browser web/programma di posta conosce le chiavi pubbliche di un insieme di enti di certificazione



Es: enti riconosciuti in Firefox



Siti certificati

- Come riconosco l'autenticità di un sito?
  - I siti che esibiscono un certificato sono segnalati dal broweser con la presenza di un lucchetto
  - Protocollo usato `https` invece di `http` e indicazione del possessore del certificato
  - Non si inseriscono password, numeri di carta di credito ecc. . . in siti senza certificato!

Section 3

Gestione del pagamento

Chi gestisce il pagamento online?

Il pagamento può essere gestito:

- Internamente: il venditore acquisisce il numero di carta di credito e trattiene la somma dovuta. Paga la commissione al gestore della carta di credito.
- Mediante terzi: il cliente paga ad un riscossore fidato il dovuto. Il venditore riceve la notifica firmata dell'avvenuto pagamento. Il venditore paga la commissione al riscossore.

Gestione interna

- Vantaggi:
  - Economicità
  - L'utente non reinserisce la carta ad ogni acquisto
- Svantaggi:
  - Rischi di sicurezza
  - Fiducia dell'utente?
  - Complicazione nella gestione del sistema

Gestione esterna

- Vantaggi:
  - Semplicità della gestione
  - Delegazione dei problemi di sicurezza
- Svantaggi:
  - Costi

Passi per la gestione esterna del pagamento

1. A effettua un acquisto dal venditore B e decide di pagare
2. B invia una *fattura* al gestore di pagamenti G
3. Il browser di A viene reindirizzato alla pagina di G che chiede il pagemento
4. A esegue il pagamento a G
5. G notifica immediatamente ad B che il pagamento è avvenuto. Il messaggio è datato e firmato
6. B verifica la firma di G e conferma l'ordine
7. Il browser di A mostra una pagina di B in cui si certifica che il pagamento è avvenuto

Gestori per il pagamento

- Paypal
- Banca Sella
- Unicredit
- ...

Riferimenti

- Wikipedia: voci *crittografia asimmetrica*, *crittografia simmetrica*, *certificato digitale*, *firma digitale*