Introduzione alla Sicurezza Web

Sommario

- Considerazioni generali
- IPSec
- Secure Socket Layer (SSL) e Transport Layer Security (TLS)
- Secure Electronic Transaction (SET)
- Introduzione alla crittografia

Considerazioni Generali (1)

- Il problema della sicurezza delle / nelle applicazioni informatiche e informazioni da queste gestite/prodotte investe diversi livelli di astrazione
  - Sensibilità dei dati
  - Diritto all'accesso alle applicazioni e alle informazioni
  - Preservare le funzionalità
  - Evitare che si verifichino danni alle persone, all'ambiente, a altri sistemi
  - …

Considerazioni Generali (2)

- Un servizio di sicurezza è un servizio di elaborazione / comunicazione fornito da un sistema allo scopo di realizzare protezione alle risorse del sistema stesso
- 5 categorie di servizi
  - Autenticazione
  - Controllo accesso
  - Riservatezza dati
  - Integrità dati
  - Non ripudio

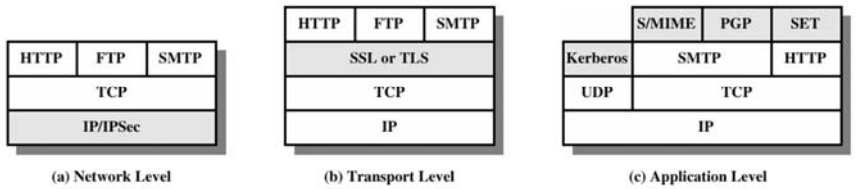
Considerazioni Generali (3)

- Dato lo scopo del corso ci concentreremo solo su alcuni aspetti che riguardano la sicurezza sul Web

Caratteristiche del Web rispetto alla sicurezza

- Il web è per definzione un insieme di risorse distribuite accessibili a tutti / molti
- È un sistema complesso
  - Nasconde debolezze che se sfruttate adeguatamente possono determinare attacchi alla sicurezza
- I server web sono facili da configurare e gestire
- Gli utenti sottovalutano i rischi

Una visione rispetto alla Pila OSI



Sicurezza a livello Rete – IPSec (1)

- È trasparente all'utente e alle applicazioni e fornisce una soluzione generale
- Comprende funzionalità di filtro
  - Solo una parte del traffico è sottoposta all'elaborazione IPSec
  - Il resto è normalmente sottoposto all'elaborazione IP

Sicurezza a livello Rete – IPSec (2)

- Permette di cifrare / autenticare tutto il traffico a livello IP
  - Si adatta a un'ampia gamma di applicazioni
- Servizi:
  - Controllo accesso
  - Integrità in assenza di connessione
  - Autenticazione sorgente
  - Rifiuto di pacchetti originati da un attacco di replay
  - Riservatezza

Secure Socket Layer – SSL

- Sviluppata da Netscape
  - inizialmente proprietaria
  - pubblica dalla versione 3
- Progettata per usare il protocollo TCP per fornire sicurezza end-to-end
- Comprende due protocolli

Architettura SSL (1)

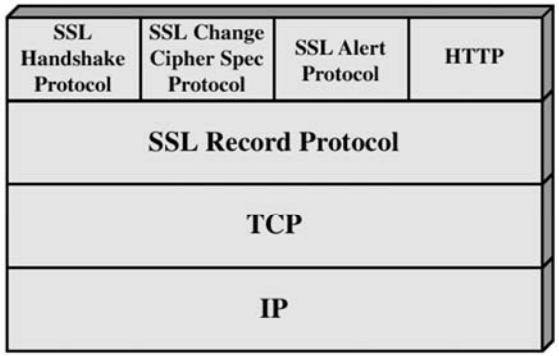
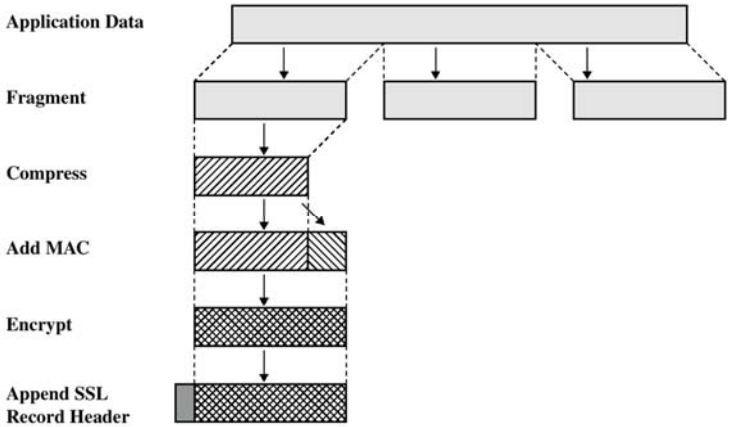


Figure 7.2 SSL Protocol Stack

Architettura SSL (2)

- Il protocollo SSL Record fornisce servizi di sicurezza di base a protocolli di livello più alto
  - HTTP opera su SSL
- I protocolli di SSL a livello più alto sono
  - Handshake
  - Change cipher spec
  - Alert
- Usati negli scambi SSL

Operazioni Protocollo SSL Record (1)



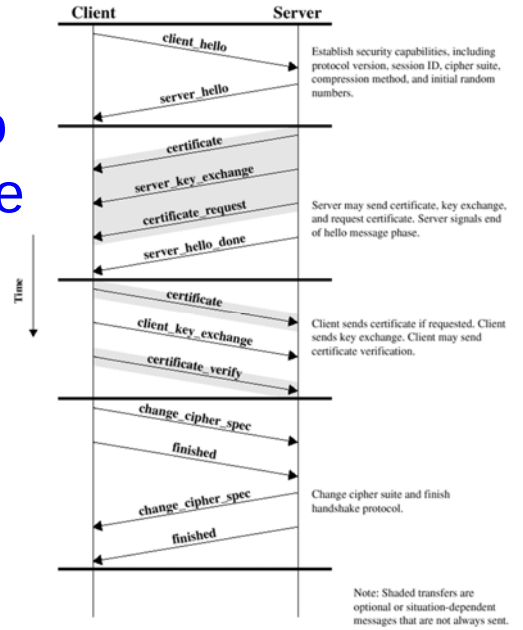
Operazioni Protocollo SSL Record (2)

- Il messaggio applicativo (dati) è frammentato in blocchi
- Ogni blocco viene eventualmente compresso ed è aggiunto un codice di autenticazione del messaggio (MAC)
- Ogni blocco è poi cifrato e viene aggiunta una specifica intestazione

Protocollo Handshake

- Permette al client e al server di autenticarsi vicendevolmente e di negoziare gli algoritmi per la cifratura e per il MAC
- Deve essere svolto prima dell'invio di qualsiasi dato dell'applicazione

Azioni del Protocollo Handshake



Transport Layer Security - TLS

- Simile a SSLv3; differenze principali:
  - Codifica dell'autenticazione del messaggio
  - Uso di funzioni pseudocasuali
  - Codici di allarme
  - Algoritmi di cifratura
  - Tipologie di certificato del client
  - …

Secure Electronic Transaction – SET

- È una specifica aperta di cifratura e sicurezza
- Progettata per transazioni con carta di credito
  - Visa, MasterCard, IBM, Microsoft, Netscape, RSA, Terisa, Verysign
- È un insieme di protocolli e formati di sicurezza, **NON** è un sistema di pagamento

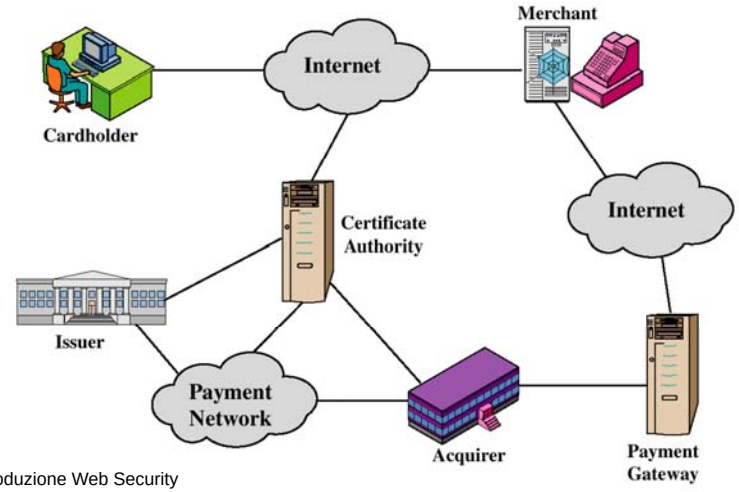
Servizi SET

- Fornisce un canale di comunicazione "sicuro" per le transazioni
- Assicura la privacy

Generalità di SET

- Confidenzialità delle informazioni
- Integrità dei dati
- Autenticazione del conto del titolare della carta di pagamento
- Autenticazione del venditore del servizio

Partecipanti a SET



Eventi in una transazione

1. Il cliente apre un conto
2. Il cliente riceve un certificato
3. Il commerciante autenticato possiede i propri certificati
4. Il cliente effettua un ordine
5. Il commerciante viene verificato
6. Vengono inviati ordine e pagamento
7. Il commerciante richiede autorizzazione al pagamento
8. Il commerciante conferma l'ordine
9. Il commerciante fornisce il bene/servizio
10. Il commerciante richiede il pagamento

Crittografia: Definizioni (1)

- Scienza che utilizza algoritmi matematici per cifrare / decifrare dati.
- Criptoanalisi = scienza che analizza e decifra i dati crittografati senza conoscerne a priori gli algoritmi utilizzati.
- Per cifrare un messaggio è necessario:
  - Un algoritmo crittografico noto
  - Una chiave (sequenza di bit) in genere segreta

Crittografia: Definizioni (2)

- Crittografia è forte/debole in funzione del tempo / risorse necessarie per ricostruire il messaggio originale da quello cifrato

Crittografia: Generalità (1)

- La sicurezza dei dati crittografati dipende da segretezza e lunghezza della chiave (# di bit)
  - e NON dall'algoritmo in genere pubblico per studiarne eventuali problemi
- La teoria dell'informazione (Shannon) dimostra che la "perfect secrecy" è ottenuta
  - con una chiave di lunghezza pari al messaggio da crittografare
  - usata una sola volta (one time pad).

Crittografia: Generalità (2)

- I sistemi crittografici utilizzati in pratica sono "computazionalmente sicuri"
  - tali per cui solo un attacco di tipo "brute-force" permetterebbe in un dato tempo di decifrare il messaggio

Classi di Sistemi di Crittografia

- Sistemi a chiave simmetrica:
  - Unica chiave per cifrare/decifrare i dati
- Sistemi a chiave asimmetrica:
  - Una chiave per cifrare, un'altra per decifrare i dati

Chiavi (1)

- La chiave è una sequenza di bit
  - Il numero di possibili combinazioni dei bit della chiave varia a seconda della sua lunghezza.
  - Una chiave lunga N bit origina 2^N combinazioni
    - 10 bit → 2^{10}=1.024
    - 20 bit → 2^{20}= 1.048.576
    - 40 bit → 2^{40}= 1.099.511.627.776
    - Chiavi di 56 bit → 2^{56}= 72.057.594.037.927.936

Chiavi (2)

- Stima delle risorse necessarie per forzare una chiave con un attacco brute force

Power / cost	40 bits (5 char)	56 bits (7 char)	64 bits (8 char)	128 bits (16 chars)
$ 2K (1 PC. Can be achieved by an individual)	1.4 min	73 days	50 years	10^{20} years
$ 100 K (This can be achieved by a company)	2 sec	35 hours	1 year	10^{19} years
$ 1 M (Achieved by a huge organization or a state)	0.2 sec	3.5 hours	37 days	10^{18} years

Fig 4 Estimate time for successful brute-force attack

Sistemi a Chiave Simmetrica (1)

- Caratteristiche
  - Velocità di esecuzione e semplice implementazione in hw
  - Lunghezza dati cifrati accettabile
- Criticità
  - Distribuzione della chiave in rete, su canale sicuro: sconsigliati per trasmettere dati in rete
- Uso
  - Cifratura dati in una macchina
  - Trasmissione dati wireless
  - PEC/Firma Digitale

Sistemi a Chiave Simmetrica (2)

- DES – Data Encryption Standard
  - Chiave a 56 bit – obsoleto
- 3DES
  - Evoluzione del DES – più robusto
- IDEA
  - chiave di 128 bit
- AES – Advanced Encryption Standard
  - chiavi di 128 o 256 bit (sostituisce il DES)
- A5
  - Usato in GSM per cifrare messaggi in fonia mobile

Sistemi Chiave Asimmetrica (1)

- Chiamati anche sistemi a Public Key Encryption o Double-Key Encryption
- Una coppia di chiavi <chiave_pubblica, chiave_privata>
- Proprietà
  - Non è possibile risalire alla chiave privata partendo dalla pubblica
  - La chiave per la cifratura non può decifrare i dati

Sistemi Chiave Asimmetrica (2)

- Principali algoritmi
  - RSA – Rivest, Shamir, Adleman
  - Diffie-Hellman
  - DSA – Digital Signature Algorithm
- Applicazioni
  - TLS (Transport Layer Security)
  - SSH (Secure Shell).
  - PEC/Firma digitale
  - Protocolli PGP e GPG (la versione Open Source OpenPGP)

Caratteristiche Sistemi Chiave Asimmetrica (1)

- La chiave pubblica serve per cifrare il messaggio
  - può essere trasmessa in rete
- La chiave privata deve essere segreta
  - è la sola che decifra il messaggio
- Se intercettato il messaggio cifrato non può essere decifrato né alterato
  - Può farlo solo il sistema in possesso della chiave privata

Caratteristiche Sistemi Chiave Asimmetrica (2)

- È garantita l'autenticazione e il non ripudio
- I fondamenti formali degli algoritmi sono riassunti in http://libeccio.dia.unisa.it/CRYPTO08/block5.pdf

Esempio

- Bob vuole inviare un msg segreto a Alice:
  - Bob richiede a Alice la sua chiave pubblica
  - Alice risponde inviandola su un canale non sicuro
  - Bob compila il msg, lo cripta usando la chiave pubblica di Alice e lo invia
  - Alice è l'unica che può decodificare il msg usando la chiave privata