

Problematiche correlate alla sicurezza informatica nel commercio elettronico



<http://www.infosec.it>

info@infosec.it

Relatore: Stefano Venturoli, General Manager Infosec

Agenda

- Cos'è il commercio elettronico
- I problemi nel commercio elettronico
- Esempi di attacchi
- Le soluzioni a nostra disposizione

Commercio elettronico o E-Commerce

- ✓ Accesso del Cliente alle Informazioni sul Prodotto
- ✓ Accesso degli utenti mobili ai sistemi interni
- ✓ Accesso dei Partner al sistema di Order Entry
- ✓ Evaluation e ricerca di Prodotto
- ✓ Accesso del Cliente ai Sistemi di Supporto
- ✓ Mercati virtuali
- ✓ Transazioni finanziarie e-Commerce
- ✓ Application Service Providers

E non solo: Informazioni a valore aggiunto

- Informazioni che generano profitto, direttamente o indirettamente
 - Informazioni
 - Programmi
 - Servizi
- Informazioni essenziali al buon funzionamento dell'azienda
 - Informazioni Operative
 - Informazioni Amministrative

Informazioni a valore aggiunto

- Informazioni riguardanti profitti futuri
 - Ricerca
 - Nuovi piani di prodotto
 - Piani Marketing
 - Database dei Clienti
- Informazioni che devono essere protette per legge
 - Dati Personali
 - Dati dei Ricercatori
 - Dati dei pazienti

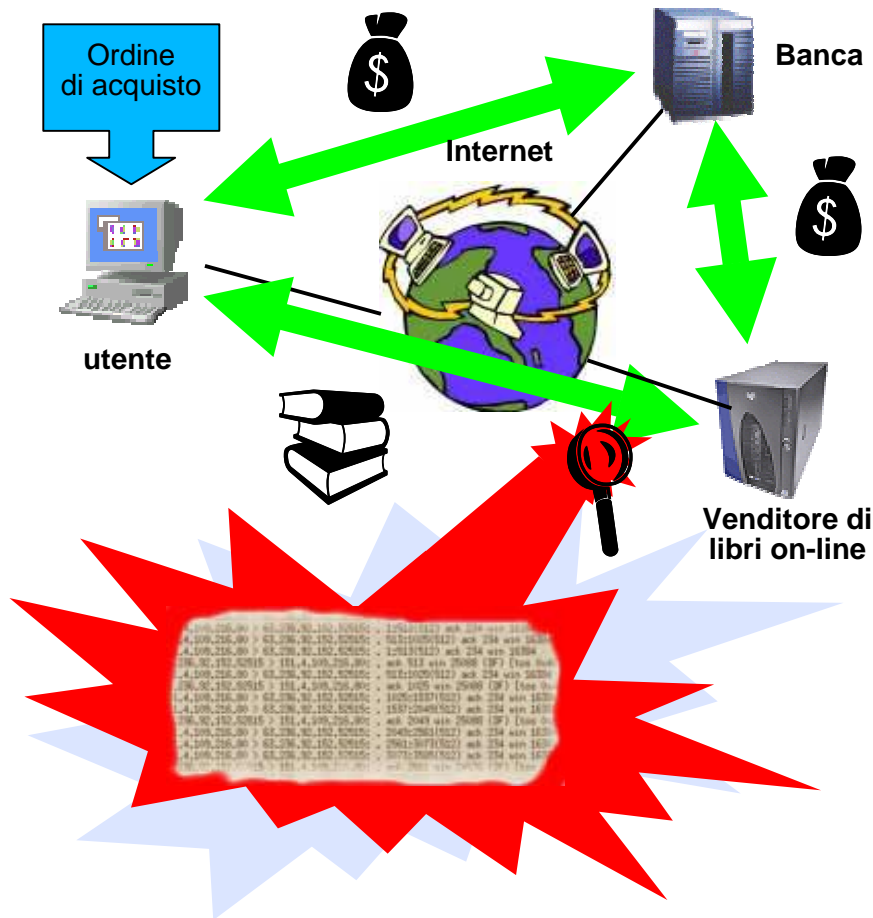
I problemi

- Sapere con chi stiamo facendo E-Commerce...
- Sapere chi ha accesso a cosa...
- Sapere che le nostre informazioni sono private...
- Sapere che il contenuto è inalterato...
- Sapere che le transazioni sono legali...
- Sapere che possiamo aver fiducia nel nostro ambiente e-commerce

L'ideale

- Autenticazione: le parti sono chi dicono di essere
- Confidenzialita' : le informazioni sensibili sono protette
- Autorizzazione: le parti per certo possono accedere solo ad informazioni a loro riservate
- Integrita': le transazioni non vengono alterate
- Non ripudio: le transazioni sono effettivamente avvenute

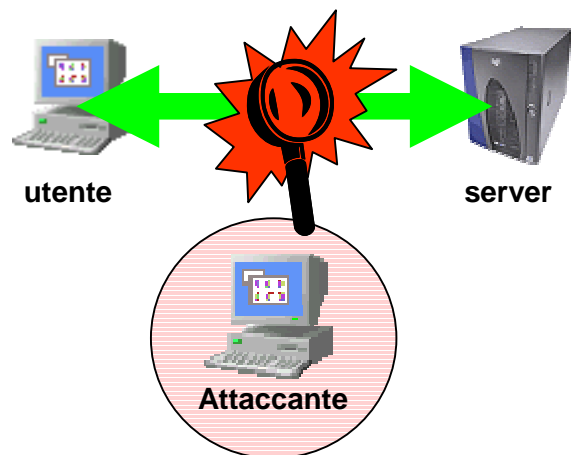
Trasmissione dei dati



Possibilità di analizzare o intercettare il traffico:

- tra utente e server e-comm.
- tra server e-comm. e banca
- tra server e database, magazzino, etc.
- tra utente e banca
- mail (di conferma, interne tra server e dipendenti o amministrazione, etc.).

Attacco MITM (Man In The Middle)

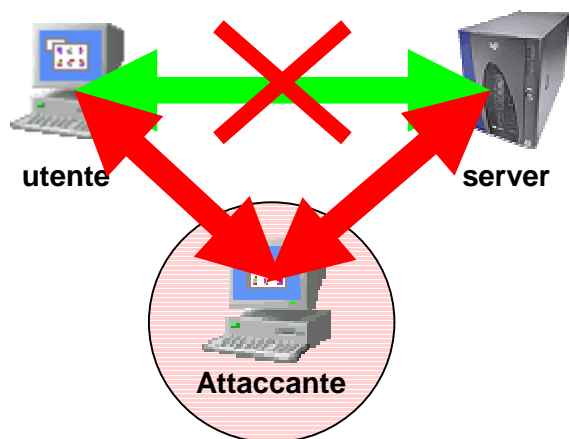


Attacco semplice (dati trasmessi in chiaro)

- estrema facilità di realizzazione
- poco attuale (almeno tra client e server e-commerce, è norma comune usare SSL)
- risolvibile usando cifratura dei dati (SSL, IPSec, PGP o S/MIME, etc.)

E' sufficiente uno "sniffer" e la possibilità di analizzare il traffico sul segmento di rete del client o del server (o in un punto qualsiasi nel percorso). Gli switch non sono una misura sufficiente a prevenire questo tipo di attacco, è necessario cifrare il traffico

Attacco MITM su SSL



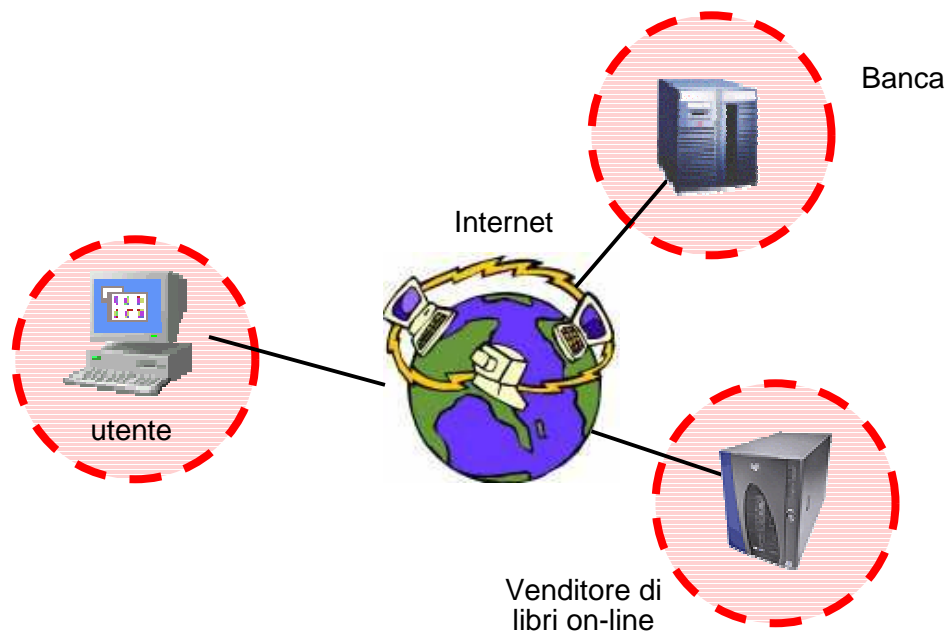
Attacco complesso (dati trasmessi cifrati)

- tool per portare questo attacco conosciuti e diffusi
- attacco molto attuale
- risolvibile verificando i certificati, per lo meno quello del server

L'attaccante simula di essere il server al quale l'utente vorrebbe collegarsi, fornendo un falso certificato.

Se l'utente non si rende conto dell'intercettazione, l'attaccante è in grado di ricevere tutti i dati, analizzarli e ritrasmetterli al server reale.

Cracking



Possibilità di analizzare o intercettare i dati:

- sul client dell'utente
- sul server di e-commerce
- su altri server collegati (database, magazzino, dipendenti, amministrazione, etc.)
- sui server della banca

Qualora non fosse possibile intercettare i dati, l'attaccante può sempre cercare di penetrare in uno dei sistemi coinvolti nella transazione, tramite le comuni tecniche di attacco da remoto.

SSL Explained

Cosa fa?

- protegge le trasmissioni
 - cifrandole
 - verificando che non siano alterate
- certifica l'identità
 - del server (se si usa una CA root riconosciuta)
 - dell'utente (se richiesto, per maggiore autenticazione, non ripudiabilità, etc.)
- integrazione PKI e token*
 - per gestione uniforme degli standard di cifratura; richiesta, emissione e revoca dei certificati; policy utenti; etc.

* Aspetti relativi all'implementazione, non allo standard.

Cosa non fa?

- **non** protegge i dati prima che vengano spediti o dopo che siano stati ricevuti
 - sul client
 - sui server
- **non** protegge da compromissioni delle PKI
 - chiavi e sistemi delle CA
 - chiavi e sistemi di server e utenti
- **non** è invulnerabile
 - errata implementazione nei software
- **non** è indecifrabile
 - sicuramente, utilizzando "weak crypto"
 - non c'è la certezza assoluta neanche con "strong crypto"
- **non** garantisce server e applicazioni
 - sistemi vulnerabili
 - errori di programmazione e configurazione
 - ...

Vulnerabilità più comuni

Server e-commerce

- servizi inutili vulnerabili
- utenti con password di default o facilmente deducibili
- servizi http o https vulnerabili
- utilizzo del server e-commerce per fornire altri servizi (ftp, mail, etc.) potenzialmente vulnerabili
- altri sistemi con relazioni "trusted" vulnerabili
- cattiva implementazione SSL (weak crypto, assenza CRL, etc.).

Software e-commerce

- cattiva o assente validazione dell'input fornito dal client in url, campi, cookie, etc.
- campi nascosti con dati sensibili/modificabili
- cookie con dati sensibili/modificabili
- cattiva gestione di ACL e metodi di accesso
- cattiva autenticazione
 - password facilmente deducibili
 - possibilità di identificarsi come utente diverso
 - cookie/sessioni che non scadono
 - modifica url e campi
 - ...

Le soluzioni

- Firma digitale
- Autenticazione sicura
- Crittografia

Si, ma quali?

Dipende dalle singole necessita'

Your Business is Internet exposed?



<http://www.infosec.it>

info@infosec.it

Noi possiamo aiutarvi