LA SICUREZZA DELLE RETI

La sicurezza in archiviazione e in trasmissione dati richiede di adottare adeguate misure per proteggere i dati da intrusi o da un loro utilizzo diverso da quello previsto dai legittimi proprietari. La tecnica di base è detta crittografia, e le 2 forme più diffuse sono simmetrica e asimmetrica, a cui sono legati argomenti come la firma digitale e la certificazione. Recentemente problema ha più peso per i pagamenti digitali, in quanto questi devono avere lo stesso livello di sicurezza di una transazione normale. Ciò è possibile implementando un set di funzionalità nel punto di accesso tra il sistema che offre i servizi e nella rete esterna, (che secondo la ISO Security Architecture) divisi in 5 classi:

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

Tutte sono sufficienti per garantire sicurezza negli scambi di informazioni tra sistema e la rete.

Autenticazione

Verifica che chi richieda un servizio sia evvettivamente quello che dichiara di essere. Gli strumenti di auth si basano sul fatto che chi deve autenticarsi deve possedere o conoscere un qualcosa di …

In un sistema di rete la trasmissione di ciò …

Controllo degli accessi

Quando l’auth è fatta, è possibile liomitare gli accessi alle sole risorse che gli possono essere assegnate.

* In caso di pc il controllo degli accessi si riferisce di solito a risorse del file system (directori, file, driver, permessi di lettura, scrittura esecuzione…)
* In caso di rete il controllo dell’accesso si basa sulla visibilità delle macchine connesse in rete e dai servizi da esse offerti, usati i firewall (vesro quali macchine far transitare pacchetti, verso quali programmi di queste, quali comandii permettere…)

Riservatezza

Quando è possibile accedere a un servizio, bisogna fare in modo che i dati che vanno tra mittente e destinatario non siano usati da terzi. Anche se è importante evitare che nessun dato sia estraibile dal traffico, la riservatezza è generalmente interpretata come protezione crittografica dei dati.

Integrità

Indipendentemente dalla riservatezza, i dati devono poter raggiungere senza modifica di terzi la destinazione. Quindi anche per info pubbliche, bisogna verificare la coincidenza di quanto ricevuto con quanto trasmesso rilevando alterazioni …

Nelle trasmissioni il codice di controllo può viaggiare non portetto, mentre nella sicurezza bisogna fare in modo che solo il mittente possa generare questo codice proteffendolo, altrimenti l’integrità dekl messaggio viene compromessa.

Non ripudio

Per le transazioni bisogna garantire che le parti di uno scambio non neghino di aver preso parte allo stesso. Si risolve con firme, elettronicamente quella digitale sem0re basata con algoritmi di crittografia.

Sicureza delle comunicazioni

Di quelle prima, auth, riservatezza e integrità riguardano aspetti generali suilla protezione delle comunicazioni

…

Sicurezza delle applicazioni

Di quelle prima, controllo degli accessi e non ripudio sono legate alle applicaazioni e interessate dallo scambio di dati. Modalità con cui si fa il controllo degli accessi sono variegate e dipendono dal sistema che si usa, dal OS dell’applicazione. Per il non ripudio invece le modalità con cui è fatta la firma digitale sono standard e le infrastrutture necessario per l’uso sono diffuse. …

Certificati digitali

Rappresentano quello che i documenti didentità costituiscono nellla vita reale; stabiliscono con esattezza lidentita delle parti. Sono dei file con valitida temportale limitata, che garantiscono l’identita di un server po una persona, usati ogni volta per problemi tipo:

* Quando si forniscono o usano servizi online ocme pagamenti e consultazione di ddati riservati,
* Quando si scambiano email, il mittente che compare non assicura un cazzo, ma lo fa la firma digitale,
* Per vaìerificare calidità di documenti da internet …

Protocollo SSL/TLS

Provvede alla sicureszza del collegamento garantendo 3 ocse:

* Privateza del collegamento: crittografia usata dopo un handshake iniziale. Per crittografare i dati si usa la crittografia simmetrica.
* Autencitazione: L’identita delle connessioni è autenticata sempre con la crittografia simmetrica …
* Affidabilità: livello trasportoo include un checo dell’integrità del messaggio basato su un MAC (Message Autentication Code) …

Il protocollo …

???

Sistema di Gestione per la Sicurezza delle Informazioni (SGSI o ?)

* …

High Level Structure

…

(foglio VM Hyperintegration, dice che ICT Security completa non è possibile, nessun ambiente è invulnerabile, e + è complesso il problema, + è difficile renderlo sicuro. Problema si verificherà anche con IOT, siccome il loro buffer è piccolo e non ci stanno sistemi e sw per protezione).

Sito MITRE attack ???

Sivaf.it/(mcnumber-cube-cybersecurity)

CWE (Common Weakness Enumeration)

Qui sono inseriti tutti gli attacchi hacker alle varie vulnerabilità e gli attacchi che si fanno.

CWE-120 o Classic Buffer Overflow

Copia del buffer di input a quello di output senza verificare input < output, causando overflow.

CLOUD COMPUING

(libro)

…

Slide - Utilizzo consapevole dei servizi

Premessa

(Esistono SaaS IaaS PaaS)

…

Per la privacy dei dati online si parla di una riflessione condivisa sia a livello europeo che a livello internazionale.

Cos’è il Cloud Computing

È un insieme di modelli di servizio che si sta diffondendo perche incoraggia un utilizzo flessibile delle proprie risorse (infrastrutture e applicazioni) o di quelle messe a disposizione da un fornitore di servizi specializzato.

Esistono 2 tipi di cloud:

* Private cloud, infrastruttura dedicata a esigenze di una singola organizzazione messa nei suoi locali o affidata alla gestione di terzi tramite *server hosting*. Sono paragonabili a datacenter aventi logiche personalizzate che ottimizzano il servizio nel tempo.
* Public cloud, l’infrastruttura invece è proprietà di un fornitore specializzato nell’erogazione di servizi che mette a disposizione degli utenti i propri sistemi erogando

Acquisire servizi cloud significa acquistare presso in fornitore di servizi … dati, infrastrutture …

…

Il problema è la pubblica amministrazione, perché in casi dove le forze dell’ordine devono accedere a dei dati per avere informazioni sensibili, essendo questi protetti da password per esempio in un IPhone, la Apple non riconosce il diritto di questi di accedere ai dati in quanto non è tenuta a seguire norme di altri paesi se non la sua aziendale.

Esternalizzare dati in cloud pubblici

Con il termine cloud computing ci si riferisce a tecnologie o servizi che:

* Favoriscono la fruizione e l’erogazione di applicazioni, capacità elaborativa e stoccaggio via web,
* Promuovono a seconda dei casi il trasferimento dell’elaborazione o della sola conservazione dei dati dai pc utenti ai sistemi del fornitore di cloud,

Geograficamente il cloud può estendersi su siti distinti anche esteri e utente potrebbe ignorare dove sono i dati. Alcuni lo dicono dove è e anche se accessibile dal mondo, chiunque che è vicino allo storage fisico potrebbe vedere dati.

…

?

1) Sicurezza informatica e privacy utenti

Usare servizi di cloud computing espone a vari problemi … (server farm non si sa dove sono?)

Nel caso di aziende, dati sono esposti a spionaggio aziendale.

2) Problemi di interazione politico-economici

… Le nazioni escluse da questa evoluzione rappresentano un problema in quanto accresce il digital divide.

Diversi modelli di servizio

Innovare, governando i rischi

Indicazioni per utilizzo consapevole dei servizi cloud