Riassunti di Crittografia - Tecnologie Internet

Simone Montali
monta.li

30 gennaio 2020

1 Concetti generali

Prima di tutto, definiamo il significato di **computer security**: la protezione applicata ad un sistema informativo con lo scopo di ottenere integrità, disponibilità e confidenzialità delle risorse. Emerge un concetto molto importante: la **CIA triad**, ossia confidenzialità, integrità, availability. (ricordiamo però altri due obiettivi: autenticità e accountability).

1.1 CIA Triad

1.1.1 Confidentiality

La confidentiality ha l'obiettivo di preservare restrizioni sull'accesso alle informazioni, inclusa la privacy personale ed informazioni proprietarie. Con **data confidentiality** intendiamo che informazioni confidenziali non sono rese visibili ad individui non autorizzati. Con **privacy** intendiamo che ogni individuo decide quali informazioni che lo riguardano rendere disponibili, e a chi.

1.1.2 Integrity

L'integrity protegge dalla modifica o distruzione di informazioni, includendo non-repudiation e authenticity. Una perdita di integrity è la modifica non autorizzata di informazioni. Con **data integrity** intendiamo l'assicurarsi che informazioni e programmi vengano cambiati in maniera definita. Con **system integrity** intendiamo l'assicurarsi che un sistema svolga le sue funzioni in maniera corretta, libero da manipolazioni.

1.1.3 Availability

Con availability intendiamo l'accesso affidabile alle informazioni. Una perdita di availability è l'interruzione dell'accesso ad alcune risorse.

1.1.4 Authenticity

Con authenticity intendiamo la proprietà, delle informazioni, di essere genuine e verificabili. In pratica, la verifica che gli utenti siano chi dicono di essere.

1.1.5 Accountability

Il goal dell'accountability è quello di poter tracciare tutte le azioni di un'entità sul sistema, in modo da riconoscere i colpevoli di un eventuale security breach.

1.2 Sfide della computer security

Elenchiamo ora alcune sfide a cui la computer security deve sopperire:

1. I requirements di sicurezza sembrano semplici, ma i meccanismi per risolverli sono complessi
2. Nello sviluppo di un meccanismo/algoritmo di sicurezza, bisogna sempre considerare i potenziali attacchi
3. Per il punto precedente, spesso le procedure necessarie sono controintuitive
4. Dopo aver progettato i sistemi di sicurezza, bisogna decidere dove utilizzarli
5. I meccanismi di sicurezza coinvolgono spesso più di un algoritmo/protocollo
6. Il vantaggio per un malintenzionato è chiaro: a lui basta trovare una sola falla, mentre il progettista deve coprirle tutte
7. C'è una naturale tendenza da parte di utenti/manager a non notare i benefici della sicurezza finché è troppo tardi
8. La sicurezza richiede monitoring costante e regolare
9. La sicurezza è spesso un aggiunta successiva alla progettazione, piuttosto che parte integrante
10. Molti utenti/amministratori vedono la sicurezza come un impedimento alle operazioni

1.3 OSI security architecture

Definiamo alcuni termini:

Security attack Ogni azione che compromette la sicurezza delle informazioni possedute da un'organizzazione

Security mechanism Un processo progettato per rilevare, prevenire e recuperare attacchi di sicurezza

Security service Un servizio che migliora la sicurezza del data processing/transfer di un'organizzazione. Sono progettati come antagonisti degli attacchi di sicurezza, e fanno utilizzo di meccanismi di sicurezza

Threat Il potenziale per una violazione di sicurezza, che esiste quando c'è una circostanza, possibilità, azione o evento che potrebbe mettere a rischio la sicurezza.

Attack Un assalto alla sicurezza di sistema che deriva da un intelligent threat, ossia un tentativo deliberato di evadere i sistemi di sicurezza.

1.4 Security attacks

Gli **attacchi attivi** coinvolgono qualche modifica del data stream, mentre quelli passivi sono di 4 tipi:

- **spoofing**: attacca l'authenticity
- **tampering**: attacca l'integrity
- **replay/reflection**: attacca l'authenticity
- **Denial Of Service**: attacca l'availability

È difficile prevenire gli attacchi attivi perché il numero di vulnerabilità è troppo alto: il goal è minimizzarne i danni.

1.5 Security service

Un **security service** è un servizio di comunicazione/processing fornito da un sistema per dare specifici tipi di protezione a risorse; implementa security policies ed è implementato da security mechanisms. Fornisce diverse tipologie di sicurezza.

1.5.1 Confidentiality

Protezione verso accesso ai dati non autorizzato. È collegato a dati ed anonimità.

1.5.2 Data integrity e message authentication

La data integrity è la proprietà che i dati non siano stati cambiati, distrutti o persi. Protegge contro modifiche non autorizzate, rilevando cambiamenti. La data origin authentication certifica la fonte di un dato, verificandone l'identità. La message authentication è l'insieme delle due cose.

1.5.3 Peer entity authentication

Fornisce la conferma dell'identità di un peer in un'associazione. Due entità sono considerate peers se implementano lo stesso protocollo in sistemi diversi. L'authentication è utilizzata nello stabilimento della connessione o durante il trasferimento. Prova a fornire anche l'assicurazione che un'entità non sia mascherata o stia replicando una connessione passata.

1.5.4 Authorization e access control

L'authorization è la verifica dei permessi su una risorsa/sistema. L'access control è l'abilità di limitare e controllare l'accesso ad un sistema.

1.5.5 System integrity and availability

La system integrity è la qualità che un sistema ha quando può eseguire la sua funzione. Si ottiene proteggendo il sistema da modifiche, perdite, distruzione. L'availability è la proprietà di un sistema di essere accessibile ed utilizzabile quando necessario, concordando con le specifiche della performance del sistema.

1.5.6 Accountability e non-repudiation

L'accountability è la proprietà di un sistema/risorsa che assicura che le azioni di un'entità siano tracciabili a quell'entità. L'**audit** è un sistema che salva informazioni necessarie all'accountability. La non-repudiation fornisce protezione verso il falso rinnego di azioni.

1.6 Meccanismi di sicurezza

I meccanismi di sicurezza hanno relazioni coi servizi; citiamo:

- Cifratura
- Firma digitale
- Access control
- Verifica dell'integrità dei dati
- Scambio di autenticazione
- Traffic padding
- Routing control
- Notarization

1.7 Principi di security design

Elenchiamo alcuni principi di security design:

Economy of mechanism Significa che il design di misure di sicurezza dovrebbe essere il più semplice possibile.

Fail-safe defaults Il concetto è basarsi sui permessi, piuttosto che l'esclusione. La situazione di default è mancanza di accesso.

Complete mediation Significa che ogni accesso deve essere verificato tramite il meccanismo di access control.

Open design Mentre le encryption keys devono essere segrete, gli algoritmi devono essere pubblici.

Separazione di privilegi Attributi di privilegio multipli sono necessari per l'accesso ad una risorsa restricted.

Least privilege Ogni processo deve operare con il numero più basso di permessi possibile.

Least common mechanism Il design deve minimizzare le funzioni utilizzate da più utenti, fornendo sicurezza mutual.

Psychological acceptability I meccanismi di sicurezza non devono interferire con il lavoro degli utenti. (least astonishment)

Isolation È un principio che si applica a tre contesti:

1. Sistemi di accesso pubblici, che devono essere isolati da risorse critiche
2. Processi e file di utenti individuali devono essere isolati gli uni gli altri
3. I meccanismi di security devono essere isolati: non dev'essere possibile accedervi

Modularity Si riferisce al separamento delle funzioni di sicurezza in moduli, ed all'architettura modulare per il design.

Layering Si riferisce all'utilizzo di approcci multipli di protezione indirizzati a persone, tecnologia, operazioni.

1.8 Attack surface e trees

Un'**attack surface** consiste nelle vulnerabilità raggiungibili di un sistema. Un **attack tree** è una struttura gerarchica ad albero che rappresenta le tecniche di exploit delle vulnerabilità.

1.9 Modello per la network security

Tutte le tecniche di sicurezza hanno due componenti: una trasformazione sulle informazioni, e un segreto condiviso. Consideriamo 4 tasks semplici per il design di un servizio:

1. Progettare un algoritmo per la trasformazione
2. Generare l'informazione segreta
3. Sviluppare metodi per la distribuzione e condivisione del segreto
4. Specificare un protocollo utilizzabile dalle entità che partecipano all'algoritmo