Azzolini Riccardo 2021-02-22

# Introduzione alla sicurezza informatica

## 1 Standard di sicurezza

Nel descrivere i vari aspetti della sicurezza informatica, è necessario adottare un modo sistematico per definire i requisiti di sicurezza e descrivere i meccanismi che possono essere utilizzati per garantire tali requisiti. A tale scopo, si fa utilizzano gli *standard di sicurezza* definiti da diversi enti internazionali, governativi e industriali. In particolare, per introdurre la sicurezza informatica è utile seguire lo standard *ITU* (International Telecommunication Union) *X.800*, "Security Architecture for OSI", il quale definisce sostanzialmente un'architettura di sicurezza di riferimento, focalizzandosi su tre aspetti: gli attacchi alla sicurezza, i servizi di sicurezza che soddisfano determinati requisiti, e i meccanismi di sicurezza impiegati per implementare tali servizi. Questo è un documento un po' datato, che non tratta alcune delle problematiche più recenti, ma è assolutamente adeguato per fare una panoramica dei fondamenti.

## 2 Attacchi alla sicurezza

Un **attacco** alla sicurezza è una qualsiasi azione che compromette la sicurezza delle informazioni in possesso di un'organizzazione (o anche di risorse hardware, ecc. — ad esempio, mandare offline un server è a tutti gli effetti un attacco). L'obiettivo della sicurezza è prevenire gli attacchi, o perlomeno scoprirli nel minor tempo possibile.

Più in generale, lo standard X.800 definisce **security threat** (minaccia alla sicurezza) qualunque minaccia che sfrutta le vulnerabilità di un sistema informativo (che esistono a causa di bug nel software, caratteristiche dei protocolli e dell'hardware impiegati, ecc.) per causare potenzialmente dei danni. Si distinguono due tipi di minacce:

- si ha una minaccia **accidentale** (*accidental threat*) quando si sfruttano in modo non intenzionale le vulnerabilità del sistema;
- si ha invece una minaccia **intezionale** (*intentional threat*), ovvero un attacco "vero e proprio", quando le vulnerabilità del sistema vengono sfruttate in modo "mirato", con l'obiettivo di comprometterne intenzionalmente la sicurezza.

Gli attacchi possono essere condotti dall'esterno o, spesso, dall'interno di un'organizzazione, e in questo secondo caso si parla di **insider threat**. Tali attacchi sono molto

comuni perché le persone all'interno di un'organizzazione hanno tipicamente più autorizzazioni rispetto a persone esterne, dunque potrebbero sfruttare tali autorizzazioni per arrecare danni più facilmente.

Un'altra distinzione presente nello standard X.800 è quella tra attacchi passivi e attivi: un attacco è **passivo** se non modifica i dati presenti/trasmessi in un sistema, mentre è **attivo** se modifica i dati o il loro flusso. Ad esempio, l'intercettazione dei messaggi e l'analisi del traffico sono attacchi passivi, mentre la riproduzione di messaggi intercettati in precedenza è un attacco attivo. Tipicamente, gli attacchi passivi sono i più difficili da scoprire.

## 3 Servizi e requisiti di sicurezza

I **servizi di sicurezza** sono servizi che migliorano la sicurezza delle informazioni di un'organizzazione, al fine di contrastare gli attacchi alla sicurezza. X.800 organizza i servizi di sicurezza secondo i requisiti di sicurezza più importanti, che sono:

- **Autenticità** (o **autenticazione**, *authentication*): assicurare che una comunicazione sia autentica. X.800 suddivide l'autenticità in due aspetti:
  - autenticità dell'**entità peer**: garantire l'identità dell'entità con cui si comunica, tipicamente al momento dell'instaurazione della comunicazione;
  - autenticità dei **dati d'origine**: garantire che tutti i dati ricevuti provengano effettivamente dall'entità con cui si vuole comunicare.
- **Segretezza dei dati** (*secrecy*): garantire la protezione dei dati durante la trasmissione.
- **Confidenzialità** (*confidentiality*, o *controllo degli accessi* nella terminologia dello standard X.800): assicurare la protezione dei dati da letture non autorizzate. Nel caso dei dati personali, si usa invece il termine **privatezza** (*privacy*), anche se questo è un problema molto più ampio, che non può essere affrontato solo con i tipici meccanismi di confidenzialità.
- **Integrità dei dati** (*data integrity*), che ha due accezioni:
  - nell'ambito del controllo degli accessi, significa proteggere i dati da modifiche non autorizzate;
  - secondo lo standard X.800, significa garantire che i dati ricevuti siano esattamente quelli inviati dall'entità comunicante.
- **Non ripudiabilità** (*non-repudiation*): proteggere contro la possibilità che una delle entità coinvolte nella comunicazione neghi di aver inviato o ricevuto un messaggio.

- **Disponibilità** (*availability*): assicurare che l'accesso ai dati non sia negato ai soggetti aventi le necessarie autorizzazioni. Un tipico esempio di attacco alla disponibilità è il *Denial of Service* (DoS), che impedisce l'accesso a un servizio, tipicamente inviando o reindirizzando un numero elevato di richieste per sovraccaricare i sistemi hardware/software che erogano il servizio.

### 3.1 CIA triad

Quando si analizza la sicurezza di un sistema informativo, si verificano tipicamente per primi tre requisiti fondamentali: confidenzialità, integrità e disponibilità. Complessivamente, questi tre requisiti prendono il nome di **CIA triad**, dalle iniziali dei termini inglesi (*Confidentiality*, *Integrity* e *Availability*).

È importante sottolineare che in questo caso, e anche in molti altri, il requisito di confidenzialità va inteso in senso più ampio rispetto alla definizione data prima, includendo in particolare anche la segretezza. Inoltre, i tre requisiti compresi nella CIA triad sono i più importanti, ma non sono affatto gli unici che devono essere considerati nell'analisi di un sistema.

Alcuni esempi di attacchi, considerati nel contesto della CIA triad, sono:

- l'*intercettazione* di un messaggio, che è una violazione della confidenzialità, intesa però come segretezza;
- l'*interruzione*, cioè impedire che un messaggio giunga a destinazione, che è una violazione della disponibilità;
- la *modifica* di un messaggio, che è una violazione dell'integrità;
- la *fabbricazione* (*fabrication*), cioè la creazione, da parte di un attaccante, di un nuovo messaggio (non derivato dalla modifica un messaggio esistente) che sembri proveniente da un'entità autorizzata; questa è una violazione dell'autenticità, un requisito che non è direttamente compreso dalla CIA triad, ma spesso viene analizzato insieme all'integrità perché è garantito dagli stessi meccanismi.

## 4 Meccanismi di sicurezza

Si definiscono **meccanismi di sicurezza** i meccanismi sviluppati per prevenire o scoprire attacchi alla sicurezza, o ripristinare il sistema dopo un attacco alla sicurezza. Alcuni esempi sono: le tecniche di cifratura, i protocolli di autenticazione, il controllo dell'accesso, i meccanismi di auditing, le procedure di recovery, ecc.

Ciascun servizio di sicurezza garantisce un determinato requisito mediante l'impiego di uno o più meccanismi di sicurezza:

- La confidenzialità è assicurata dal *meccanismo di controllo dell'accesso*.
- La segretezza è ottenuta tramite le *tecniche di cifratura*.
- L'integrità, nelle sue due accezioni, è assicurata dal *meccanismo di controllo dell'accesso* e dalle *tecniche di cifratura*. Inoltre, si può considerare anche una terza accezione di integrità, intesa come correttezza semantica dei dati, che è garantita dai *vincoli di integrità*.
- La disponibilità è assicurata dalle *tecniche di recovery* e dai *sistemi anti denial of service*.
- L'autenticità e la non ripudiabilità sono assicurate dalle tecniche di *firma digitale* e dai *protocolli di autenticazione*.

In generale, l'implementazione dei servizi di sicurezza varia a seconda che si consideri la sicurezza delle informazioni quando esse risiedono nel sistema informativo o quando vengono trasmesse.