Università degli studi di Perugia
Facoltà di Ingegneria

Appunti di Sicurezza Informatica

Burani Alessio

Anno Accademico 2014/2015

Indice

1 Introduzione alla sicurezza informatica **2**
1.1 Premessa 2
1.1.1 Definizione 2
1.2 Concetti fondamentali 2
1.2.1 Sistema informativo e informatico 2
1.2.2 Vulnerabilità, Minacce, Attacchi, Difesa 3
1.2.3 Sicurezza informatica: definizione classica e requisiti CIA 4
1.2.4 Requisiti AAA 6
1.2.5 Tipologie di Minacce e Attacchi 7
1.2.6 Principi della Sicurezza Informatica 8
1.3 Fondamenti di Crittografia 9

Capitolo 1

Introduzione alla sicurezza informatica

1.1 Premessa

1.1.1 Definizione

Che cosa significa sicuro? La parola sicurezza e l'aggettivo sicuro vengono sempre associati a beni che si desidera proteggere da possibili danni, danneggiamenti, perdita, e via dicendo. In particolare un bene è al sicuro se è ben protetto, e la sua messa in sicurezza non deve impedirne l'utilizzo. Esistono molteplici definizioni di sicurezza informatica, ad esempio:

- Security is the degree of protection against danger, damage, loss, and criminal activity [2].
- Security is a form of protection where a separation is created between the assets and the threat [1].

La parola sicurezza deriva dal latino sine cura: senza preoccupazione. La sicurezza di un sistema può essere definita come la conoscenza del fatto che l'evoluzione del sistema non produrrà stati indesiderati. Le cause che possono minare la sicurezza sono molteplici e spesso non prevedibili, quindi non si può parlare di sicurezza in senso assoluto, ma solo relativo (*L'unico computer sicuro è un computer spento*).

Trasversalità della tematica: Le problematiche di sicurezza interessano molteplici campi (attività lavorative, vita domestica, hobby, giochi, sport, etc.). Di fatto, ogni settore della vita moderna ha delle implicazioni relative alla sicurezza. Il livello di sicurezza di un'organizzazione dipende dai livelli di sicurezza di tutti i suoi comparti/settori. Il livello di sicurezza di un sistema è determinato dal livello di sicurezza dal suo comparto meno sicuro (principio dell'anello debole).

1.2 Concetti fondamentali

1.2.1 Sistema informativo e informatico

- Per sistema informativo (information system) di un'organizzazione si intende l'insieme delle informazioni prodotte ed elaborate e delle risorse umane, materiali e immateriali, coinvolte nel processo di elaborazione di tali informazioni
- Per sistema informatico (information and communication technology system) s'intende l'insieme delle varie tecnologie coinvolte nel sistema informativo (il sistema informativo è parte del sistema informatico).

Questo corso verterà sulla sicurezza dei sistemi informativi. Tuttavia, si approfondiranno maggiormente questioni inerenti la sicurezza dei sistemi informatici. Per sicurezza di un sistema

informativo si intende il grado di protezione contro qualsiasi minaccia ai suoi asset. Richiede il soddisfacimento dei seguenti requisiti:

- **confidenzialità, integrità e disponibilità**
- **assicurazione, autenticità e anonimato**

Quando si parla di **attacco** solitamente si intende la violazione di uno o più di questi requisiti.

1.2.2 Vulnerabilità, Minacce, Attacchi, Difesa

Vulnerabilità

Una vulnerabilità (o falla o breccia) è una **debolezza intrinseca** di un sistema, che potrebbe essere sfruttata per provocare perdite o danni. Scaturisce spesso da errate procedure di sicurezza e/o da errori di progettazione/implementazione, e in alcuni casi è intimamente legata alla natura del sistema. Ad esempio:

- un sistema potrebbe essere vulnerabile alla manipolazione non autorizzata dei dati causa un bug nella procedura di autenticazione dell'utente
- un calcolatore è vulnerabile all'acqua

Nel primo caso (vulnerabilità scaturite da errate procedure di sicurezza) l'insorgenza delle vulnerabilità può essere mitigata adottando adeguati standard e norme di qualità.

Minacce (Threats)

Per minaccia (threat) ad un sistema informatico/informativo si intende quell'insieme di circostanze che potrebbero arrecare danni ai suoi asset: eventi potenziali, accidentali o deliberati, che, nel caso accadessero, produrrebbero perdite e danni. il realizzarsi di una minaccia generalmente avviene sfruttando una o più vulnerabilità del sistema. Si parla quindi di situazioni ipotetiche che potrebbero avvenire in determinate circostanze. Ad esempio:

- esecuzione di codice malevole che invia dati sensibili ad un'organizzazione criminale
- accesso a dati riservati da parte di entità non autorizzate
- perdita di dati a causa della rottura di un apparato hardware o al crash di uno specifico software

Attacchi (Attacks)

Un attacco (attack) è un atto deliberato teso ad arrecare un danno al sistema. Consiste, di fatto, nella realizzazione di una **minaccia**. Generalmente, un attacco viene perpetrato attraverso lo sfruttamento di una o più vulnerabilità. Spesso si classificano in base all'entità del danno:

- **attacco attivo (active attack)**: altera le risorse o ne modifica il processo di gestione/elaborazione
- **attacco passivo (passive attack)**: ottiene le informazioni/dati senza alterarli e senza modificare il relativo processo di gestione/elaborazione

Un'altra importante classificazione è in base al luogo da cui viene iniziato l'attacco:

- **attacco dall'interno (inside attack)**: attacco iniziato da un'entità all'interno del perimetro di sicurezza di un sistema informativo di una data organizzazione
- **attacco dall'esterno (outside attack)**: attacco iniziato da un'entità all'esterno del perimetro di sicurezza

Ovviamente, è molto più difficile prevenire e rilevare gli attacchi interni di quelli esterni. Ciò anche a causa del fatto che le misure di prevenzione per questo tipo di attacchi limita notevolmente l'usabilità del sistema (si pensi, ad esempio, alla struttura gerachica in ambiente militare, in cui ogni risorsa conosce il minimo indispensabile per svolgere i propri compiti. In questo modo nel caso la risorsa venga compromessa, si limita il danno. Ovviamente tutto ciò rallenta il processo di funzionamento del sistema).

Tecniche di difesa

Diverse contromisure (o misure protettive) possono essere attuate per proteggere un sistema informativo da eventi accidentali e da attacchi deliberati. Tali misure devono essere strutturate all'interno di un piano di sicurezza redatto dopo un'attenta analisi costi/benefici (textitcost-effective solutions). Le tecniche di difesa possono essere di tipo:

- **preventivo**: effettuano una serie di **controlli** per evitare **a priori** che attacchi noti o immaginabili possano essere sferrati con successo (e.g. controlli aeroportuali, controllo di accessi e permessi negli OS).
- **a posteriori**: sono tese a ridurre gli effetti di un attacco che è riuscito a eludere le misure preventive di cui sopra; devono monitorare un sistema ed essere in grado di **rivelare** comportamenti anomali.

Un **meccanismo di sicurezza** è un qualsiasi metodo, strumento, o procedura teso a rilevare, prevenire o porre rimedio agli effetti di un attacco alla sicurezza del sistema. La strategia di difesa, qualunque essa sia, combina in modo opportuno uno o più meccanismi di sicurezza. molti meccanismi di sicurezza consistono in controlli hardware/software.

1.2.3 Sicurezza informatica: definizione classica e requisiti CIA

La sicurezza informatica si fonda sulla protezione dei seguenti macro-requisiti di un sistema informativo (informatico):

- **Confidenzialità (Confidentiality)**
- **Integrità (Integrity)**
- **Disponibilità (Availability)**

Spesso si utilizza l'acronimo C.I.A. per denotarli in modo compatto. Ovviamente, come si può

Figura 1.1: Diagramma di Venn dei macro-requisiti di sicurezza

notare dal diagramma di Venn in Figura 1.1 spesso vengono richiesti contemporaneamente più di questi requisiti, cosi come un attacco può violare più requisiti.

Confidenzialità (Confidentiality)

Def. **Confidentiality**: the property that information is not made available or disclosed to unauthorized individuals, entities, or processes. Per confidenzialità si intende quindi la garanzia che alle risorse informatiche accedano solo le parti autorizzate ad accedervi. E' talvolta denominata segretezza, riservatezza o privacy. Nota bene: per accesso non si intende solo la lettura, ma anche la visualizzazione, la stampa o la semplice consapevolezza dell'esistenza di una data risorsa nel sistema.

Attacchi alla confidenzialità: Si ha un attacco alla confidenzialità quando una entità (persona, processo o risorsa) tenta di accedere senza autorizzazione a informazioni protette (mentre queste sono memorizzate, oppure durante l'elaborazione, oppure ancora durante una comunicazione). La protezione della confidenzialità avviene utilizzando in modo appropriato i seguenti strumenti (meccanismi) di sicurezza informatica:

- **Cifratura (Encryption)**
- **Controllo degli accessi (Access Control)**
- **Sicurezza fisica (Physical security)**

Integrità (Integrity)

Def. **Integrity**: safeguarding the accuracy and completeness of information and processing methods.
Def. **Integrity**: the property of safeguarding the accuracy and completeness of assets.

Per integrità si intende quindi la garanzia che le risorse possano essere modificate solo dalle parti autorizzate e solo nei modi prestabiliti. Le modifiche comprendono la scrittura, la variazione, il cambiamento dello stato, l'eliminazione e la creazione. Nel caso di file, conviene includere anche i metadati associati (proprietario, ultimo utente ad averlo letto, data ultima modifica,data di creazione), in modo che un accesso non autorizzato al contenuto possa essere rivelato da un controllo di integrità applicato ai metadati.

Attacchi all'integrità: Si ha un attacco all'integrità quando una entità (persona, processo o risorsa) tenta di modificare senza autorizzazione una o più risorse del sistema informativo.

La protezione della confidenzialità avviene utilizzando in modo appropriato i seguenti strumenti (meccanismi) di sicurezza informatica (tutti basati su un uso corretto della ridondanza):

- **Backup**
- **Somma di controllo o Checksum**
- **Codici a correzione di errore (Corruzioni non deliberate ma accidentali, possono essere facilmente elusi da attacchi intelligenti)**
- **Codici di autenticazione dei messaggi o Message Authentication Code MAC**

Disponibilità (Availability)

Def. **Availability**: ensuring that authorized users have access to information and associated assets when required.

Per disponibilità (availability) si intende quindi che le risorse siano accessibili, nei tempi e nei modi prestabiliti, alle parti autorizzate ogni volta che le richiedono: se una persona o un sistema dispone dei diritti di accesso ad una risorsa, l'accesso non deve essergli impedito. Spesso la disponibilità viene citata tramite il suo opposto: la **negazione di servizio** (**Denial of Service** o **DoS**). La disponibilità può assumere significati/sfumature diverse; una risorsa può trovarsi in uno stato intermedio tra i due opposti stati di piena disponibilità e di piena indisponibilità.

Conflittualità requisiti CIA

Spesso i requisiti di confidenzialità, integrità e disponibilità possono essere in conflitto tra loro. E' quindi importante trovare il compromesso ottimo per la garanzia di tutti e tre. E' facile garantire la confidenzialità di una risorsa impedendo a chiunque di accedervi (e.g. se chiudo la risorsa in un blocco di cemento, sicuramente resterà confidenziale. Tuttavia la disponibilità della stessa verrebbe compromessa in senso assoluto).

1.2.4 Requisiti AAA

In aggiunta ai concetti CIA, sovente viene richiesto il soddisfacimento di ulteriori requisiti che vanno sotto l'acronimo A.A.A.

Assicurazione (Assurance)

Per assicurazione (assurance) si intende come viene fornita e gestita la fiducia reciproca tra le varie parti coinvolte nel sistema informativo. Tale requisito sopperisce la mancanza di regolamentazione, da parte dei requisiti C.I.A., dell'uso delle risorse di un sistema. E' teso quindi ad evitare un uso non consono dei vari asset del sistema. Tale concetto è ovviamente bidirezionale: così come il sistema deve fidarsi degli utenti (del fatto che non lo usino in modo inappropriato), gli utenti devono fidarsi del sistema (e.g.:trattamento dei dati personali). Il concetto di fiducia è tuttavia difficile da quantificare ed è legato al grado di confidenza sul comportamento che ci si attende dal sistema. Il requisito di assicurazione viene regolato agendo sui seguenti strumenti:

- **Politiche (Policies):** specifiche comportamentali che regolano l'operato degli attori del sistema
- **Permessi (Permissions):** descrivono le operazioni ammesse/concesse e quelle proibite
- **Protezioni (Protections):** implementazione dei meccanismi di sicurezza tesi ad applicare e far rispettare le politiche e i permessi di cui sopra
- **Qualità del software:** lo sviluppo del software che rispetta standard di qualità rigorosi rende più difficile che il sistema si discosti dai comportamenti attesi

Autenticità (Authenticity)

L'autenticità è la capacità di provare che dichiarazioni, politiche e autorizzazioni rilasciate da persone o sistemi siano veritiere. Se non è garantita persone/sistemi possono sostenere argomentazioni non vere senza essere contraddetti da prove oggettive. Se è garantita, si dice anche che è soddisfatto il requisito del textbfnon-ripudio (non-ripudiation). Per non-ripudio si intende che dichiarazioni autentiche rilasciate da persone e/o sistemi NON possono essere negate. La firma digitale è il principale meccanismo crittografico che permette di ottenerlo. Un contesto in cui tale requisito è importante è, ad esempio, la PEC.

Anonimato (Anonymity)

Per anonimato (anonymity) si intende che non è possibile ottenere o risalire all'dentità di un individuo pur avendo accesso a determinati record/transazioni di un sistema informativo. Se un'organizzazione deve rendere pubblici alcuni dati dei suoi clienti/membri senza violarne la privacy, può adottare alcuni dei seguenti strumenti:

- **Aggregazione (Aggregation):** combinare mediante somme e/o medie i dati di diversi individui
- **Miscelazione (Mixing):** permutare i dati dei singoli utenti in modo da preservare l'esito di predeterminate query
- **Mediazione (Proxies):** utilizzare degli agenti fidati che si interpongono tra l'individuo e i sistemi con i quali interagisce

- **Pseudonimi (Pseudonyms):** utilizzare delle identità fittizie eventualmente autenticate da una terza entità che funge da garante

1.2.5 Tipologie di Minacce e Attacchi

E' possibile classificare diverse minacce e attacchi rispetto a quali requisiti violano. Vediamone alcune:

Intercettazione (Eavesdropping)

Si ha un'intercettazione quando un'entità non autorizzata ha ottenuto l'accesso ad una risorsa. Generalmente questo tipo di attacchi avviene nella fase di trasmissione dell'informazione, e rappresenta una violazione alla confidenzialità. Esempi:

- copia illecita di file di programma o dati
- intercettazione di una comunicazione telefonica
- sniffing di pacchetti di dati

Un'intercettazione potrebbe essere molto difficile da rilevare, poiché un intercettatore "silenzioso" potrebbe essere molto abile e non lasciare tracce o concellarle.

Alterazione (Alteration)

Si ha una alterazione o modifica quando un'entità non autorizzata, oltre ad accedere a una risorsa, interferisce con essa modificandola. Rappresenta una violazione alla confidenzialità. Esempi:

- attacchi di tipo textbfman-in-the-middle: un flusso di dati viene intercettato, modificato e ritrasmesso (rappresenta anche una minaccia alla confidenzialità)
- virus informatici che modificano file di sistema critici in modo da eseguire azioni maliziose
- cambiare i valori di un database o modificare un programma in modo che esegua dei calcoli diversi

Alcuni casi di alterazione possono essere facilmente rilevati, mentre altre modifiche, più sottili, possono essere estremamente difficili da individuare.

Interruzione (Denial-of-service)

In un'interruzione, una risorsa del sistema viene degradata o eliminata, diventando non disponibile o inutilizzabile. Rappresenta una minaccia alla disponibilità e/o all'integrità. Esempi:

- la distruzione o il sabotaggio di un dispositivo
- la cancellazione di un file
- la congestione di un Web server causata da un numero enorme di richieste artificiali

Falsificazione (Masquerading)

La falsificazione consiste nella contraffazione di risorse (dati/hardware) da parti non autorizzate. Costituisce principalmente una violazione di autenticità, e a volte anche alla confidenzialità e/o all'integrità. Esempi:

- phishing: creazione di siti Web apparentemente identici agli originali allo scopo di frodarne gli utenti
- textbfspoofing: spedizione di pacchetti dati con falsi indirizzi di ritorno

A volte le falsificazioni sono facilmente rilevabili, ma se attuate con abilità potrebbero essere del tutto indistinguibili da normali operazioni reali legittime.

Ripudio (Ripudiation)

Il ripudio consiste nel negare di aver effettuato una data azione. Ll'azione potrebbe essere la ricezione o la spedizione di un messaggio, così come l'esecuzione di una transazione. Spesso, riguarda il tentativo di recedere da un contratto (accordo) precedentemente assunto in cui era comunque previsto l'uso di ricevute (o simili) per dimostrare l'esecuzione di determinate operazioni. Si tratta di un attacco all'assicurazione.

Inferenza (Inference), Correlation and traceback

Per inferenza o attacco inferenziale si intendono un insieme di tecniche che utilizzando la statistica e l'algebra permettono di ricavare/stimare **informazioni sensibili** a partire da dati non sensibili. Rappresenta un attacco alla confidenzialità, e spesso è attuato nel contesto dei databases. Similmente, per correlation and traceback si intendono un insieme di tecniche basate sulla statistica e sull'algebra che permettono di determinare la sorgente di una particolare informazione o di un particolare flusso di dati.

N.B.: C'è una differenza, in senso giuridico, tra dati personali e dati sensibili. Tale distinzione dipende dalla giurisdizione dei paesi. In particolare in Italia il dato personale viene indicato come un'informazione che permette di identificare un individuo (anagrafica), mentre un dato sensibile rappresenta un'informazione su aspetti della vita privata dell'individuo (orientamento sessuale, opinione politica, credo religioso, etc.)

1.2.6 Principi della Sicurezza Informatica

Mediazione completa (Complete mediation):

Ogni accesso ad una risorsa deve essere controllato verificando che sia conforme alle politiche di sicurezza stabilite; diffidare da miglioramenti nell'efficienza ottenuti salvando autorizzazioni precedentemente acquisite, poiché i permessi possono variare nel tempo.

Struttura aperta (Open design):

L'architettura, il progetto e l'implementazione dei meccanismi di sicurezza di un sistema devono essere resi pubblici.

- la sicurezza deve fondarsi sulla segretezza di pochi elementi chiave
- maggior feedback favoriscono l'individuazione di bug, falle e vulnerabilità, aumentando la robustezza e la sicurezza del sistema
- un meccanismo di protezione ritenuto sicuro da molti è preferibile ad uno noto solo a pochi. E' quindi bene evitare meccanismi di sicurezza basati sulla segretezza (security by obscurity).

Separazione dei privilegi (Separation of privilege):

Più condizioni dovrebbero essere richieste per concedere l'accesso a risorse limitate o ottenere il permesso di effettuare una data azione. In genere questo principio comporta una separazione logico/funzionale delle componenti di un sistema.

Minimo privilegio (Least privilege):

Ogni parte di un sistema deve avere i privilegi minimi necessari allo svolgimento dei propri compiti. Per attività inusuali che richiedono maggiori privilegi conviene assegnare autorizzazioni temporanee fortemente limitate nel tempo. In questo modo si riduce il rischio di attacchi basati sulla scalata di privilegi.

Minimo meccanismo comune (Least common mechanism):

I meccanismi di sicurezza che per l'accesso e la gestione di risorse condivise non dovrebbero essere a loro volta condivisi o dovrebbero essere condivisi il meno possibile. E' quindi buona norma adottare tecniche di isolamento quali la virtualizzazione e il sandboxing (e.g. browser web: nessuna applicazione web può agire sul filesystem, eccetto attraverso i cookies). In questo modo vengono mitigati rischi derivanti da comportamenti malevoli di utenti cui spetta comunque l'accesso a una data risorsa condivisa.

Usabilità (Usability, Psychological acceptability):

I meccanismi di sicurezza non devono rendere più difficile l'accesso alle risorse. Le interfacce utente devono essere ben progettate, intuitive e di facile utilizzo, mentre i parametri di configurazioni inerenti aspetti di sicurezza devono essere di semplice comprensione e facilmente modificabili.

Fattore lavoro (Work factor):

Il costo necessario ad aggirare un meccanismo di sicurezza deve essere confrontabile alle risorse di cui dispone un potenziale attaccante. Un meccanismo di sicurezza deve avere un livello di sofisticazione, e pertanto un costo, che tenga conto del valore degli asset da proteggere e delle risorse a disposizione di potenziali attaccanti.

Monitoraggio (Compromise recording):

A volte può convenire effettuare un monitoraggio dettagliato piuttosto che investire in sofisticati meccanismi di sicurezza di tipo preventivo.

Penetrazione più semplice:

un attaccante utilizzerà qualsiasi mezzo di penetrazione disponibile: non necessariamente i mezzi più ovvi (prevedibili), non necessariamente i mezzi per i quali sono state installate le difese più solide. (e.g.: E' inutile avere un sistema informatico sicuro se il personale non viene formato e fornisce a chiunque credenziali di accesso). L'applicazione di tale principio presenta le seguenti difficoltà:

- saper anticipare l'avversario, cioè riuscire a prevederlo
- gestire in modo equilibrato la sicurezza delle diverse parti di un sistema; rafforzare le difese di una parte può indurre gli avversari ad attaccare un'altra parte (più debole) del sistema.

Temporalità:

le risorse di un sistema informativo devono essere protette solo fino a quando possiedono un valore, e in modo proporzionale al loro valore. Generalmente tale principio si riferisce ai dati: il loro valore può subire brusche variazioni; si consideri ad esempio il valore dei dati sull'andamento dei mercati prima e dopo la loro divulgazione.

Anello più debole:

la sicurezza di un sistema articolato NON può essere più forte del suo anello più debole. La gestione della sicurezza deve tener conto del sistema nel suo insieme. Un elevato grado di sicurezza delle singole parti non implica un elevato grado di sicurezza globale, ma è necessario prevedere anche una strategia oculata di coordinamento della varie parti che non introduca vulnerabilità (l'insieme è più della somma delle parti).

1.3 Fondamenti di Crittografia

Bibliografia

[1] [ISECOM]. http://www.isecom.org.

[2] [wiki en]. http://en.wikipedia.org/wiki/security.