18/10

**NETWORK SECURITY**

**Cybersecurity**

La sicurezza informatica è la protezione delle informazioni archiviate, trasmesse ed elaborate in un sistema in rete di computer, altri dispositivi digitali, dispositivi di rete e linee di trasmissione, inclusa Internet.

La protezione comprende riservatezza, integrità, disponibilità, autenticità e accountability.

I metodi di protezione includono:

* politiche e procedure organizzative
* mezzi tecnici quali la crittografia e i protocolli di comunicazione sicuri

La componente umana …

Come sottoinsiemi della sicurezza informatica, possiamo definire:

* Sicurezza delle informazioni: questo termine si riferisce alla preservazione della riservatezza, dell'integrità e della disponibilità di informazioni. Inoltre, possono essere coinvolte anche altre proprietà, come l’autenticità, l’accountability, il non ripudio e l’affidabilità
* Sicurezza della rete: questo termine si riferisce alla protezione delle reti e del loro servizio da modifiche, distruzioni o divulgazioni non autorizzate e alla garanzia che la rete esegue correttamente le sue funzioni critiche e non vi sono effetti collaterali dannosi

**Obiettivi di sicurezza**

La definizione di sicurezza informatica introduce 3 obiettivi chiave, ovvero la triade della CIA:

* **Riservatezza**: questo termine copre due concetti correlati:
  + Riservatezza dei dati: garantisce che le informazioni private o riservate non siano rese disponibili o divulgate a soggetti non autorizzati.
  + Privacy: garantisce che gli individui controllino o influenzino quali informazioni a loro relative possono essere raccolte e archiviate e da chi e a chi tali informazioni possono essere divulgate.
* **Integrità**: questo termine copre due concetti correlati:
  + Integrità dei dati: garantisce che i dati (sia archiviati che nei pacchetti trasmessi) e i programmi vengano modificati solo in un modo specificato e autorizzato.

Questo concetto comprende anche:

* + - autenticità dei dati, il che significa che un oggetto digitale è effettivamente ciò che afferma di essere o ciò che si afferma di essere
    - non ripudio, ovvero la garanzia che al mittente delle informazioni venga fornita la prova della consegna e al destinatario venga fornita la prova dell'identità del mittente, in modo che nessuno dei due possa successivamente negare di aver elaborato le informazioni.
  + Integrità del sistema: garantisce che un sistema svolga la funzione prevista in modo inalterato, esente da manipolazioni non autorizzate deliberate o involontarie del sistema
* **Disponibilità**: garantisce che i sistemi funzionino tempestivamente e che il servizio non venga negato agli utenti autorizzati

Lo standard NIST FIPS 199 (Standards for Security Categorization of Federal Information and Information Systems) elenca la riservatezza, l'integrità e la disponibilità come i tre obiettivi di sicurezza per le informazioni e i sistemi informativi.

FIPS 199 fornisce un'utile caratterizzazione degli obiettivi della CIA in termini di:

* requisiti
* definizione di una perdita di sicurezza in ciascuna categoria

Confidenzialità:

* Preservare le restrizioni autorizzate sull'accesso e sulla divulgazione delle informazioni, compresi i mezzi per proteggere la privacy personale e le informazioni proprietarie.
* Una perdita di riservatezza è la divulgazione non autorizzata di informazioni.

Integrità:

* Protezione contro la modifica o la distruzione impropria delle informazioni, inclusa la garanzia del non ripudio e dell'autenticità delle informazioni.
* Una perdita di integrità è la modifica o la distruzione non autorizzata delle informazioni.

Disponibilità:

* Garantire un accesso e un utilizzo tempestivo e affidabile delle informazioni
* Una perdita di disponibilità è l'interruzione dell'accesso o dell'utilizzo delle informazioni o di un sistema informativo

**Obiettivi aggiuntivi**

Autenticità:

* La proprietà di essere autentici e di poter essere verificati e affidabili
* Fiducia nella validità di una trasmissione, di un messaggio o del mittente del messaggio
* Ciò significa verificare che gli utenti siano chi dicono di essere e che ogni input che arriva al sistema provenga da una fonte attendibile

Accountability:

* L'obiettivo di sicurezza che genera il requisito che le azioni di un'entità siano riconducibili in modo univoco a tale entità
* Ciò supporta il non ripudio, la deterrenza, l'isolamento dei guasti, il rilevamento e la prevenzione delle intrusioni, il ripristino post-azione e l'azione legale.
* Poiché i sistemi veramente sicuri non sono ancora un obiettivo raggiungibile, dobbiamo essere in grado di risalire a una violazione della sicurezza fino alla parte responsabile
* I sistemi devono tenere traccia delle proprie attività per consentire successive analisi forensi per individuare violazioni della sicurezza o per facilitare le controversie sulle transazioni

**Obiettivi di sicurezza**

Immagine che contiene testo, schermata, Carattere, biglietto da visita

Descrizione generata automaticamente

**Sfide di sicurezza**

1. La sicurezza non è così semplice come potrebbe sembrare a un principiante.

I requisiti sembrano essere semplici. Alla maggior parte dei principali requisiti per i servizi di sicurezza possono essere assegnate etichette autoesplicative composte da una sola parola:

riservatezza, autenticazione, non ripudio e integrità

I meccanismi utilizzati per soddisfare tali requisiti possono essere piuttosto complessi. Comprenderli può richiedere un ragionamento piuttosto sottile.

1. Nello sviluppo di un particolare meccanismo o algoritmo di sicurezza, è necessario sempre considerare i potenziali attacchi a tali funzionalità di sicurezza.

In molti casi, gli attacchi riusciti vengono progettati considerando il problema in un modo completamente diverso sfruttando una debolezza inaspettata del meccanismo.

1. A causa di 2, le procedure utilizzate per fornire particolari servizi sono spesso controintuitive.

In genere, un meccanismo di sicurezza è complesso. Dall'enunciazione di un requisito particolare non risulta evidente che siano necessarie misure così elaborate. È solo quando si considerano i vari aspetti della minaccia che ha senso elaborare meccanismi di sicurezza

Poi disegno slide

1. Dopo aver progettato vari meccanismi di sicurezza, è necessario decidere dove utilizzarli.

Questo è vero sia in termini di:

* posizionamento fisico: ad esempio, in quali punti di una rete sono necessari determinati meccanismi di sicurezza
* collocazione logica: ad esempio, a quale livello o livelli di un'architettura dovrebbero essere collocati i meccanismi

1. I meccanismi di sicurezza in genere coinvolgono più di un particolare algoritmo o protocollo.

Richiedono inoltre che i partecipanti siano in possesso di alcune informazioni segrete (ad esempio, una chiave di crittografia). Ciò solleva interrogativi sulla creazione, distribuzione e protezione di tali informazioni segrete.

Potrebbe anche essere necessario fare affidamento su protocolli di comunicazione il cui comportamento potrebbe complicare il compito di sviluppare il meccanismo di sicurezza. Se il corretto funzionamento del meccanismo di sicurezza richiede la fissazione di limiti di tempo sul tempo di transito di un messaggio dal mittente al destinatario, allora qualsiasi protocollo o rete che introduca ritardi variabili e imprevedibili potrebbe rendere tali limiti di tempo privi di significato.

1. La sicurezza delle informazioni e della rete è essenzialmente una battaglia di ingegno tra un autore del reato che cerca di trovare buchi e il progettista o l'amministratore che cerca di chiuderli.

Il grande vantaggio che ha l'attaccante è che gli basta trovare un solo punto debole, mentre il progettista deve trovare ed eliminare tutti i punti deboli per ottenere una sicurezza perfetta (??)

1. Esiste una tendenza naturale da parte degli utenti e dei gestori di sistema a percepire scarsi benefici dagli investimenti in sicurezza

fino a quando non si verifica un errore di sicurezza

1. La sicurezza richiede un monitoraggio regolare, persino costante.

Ciò è difficile nell’ambiente sovraccarico e a breve termine di oggi.

Questo è costoso.

1. La sicurezza è ancora troppo spesso un aspetto secondario da incorporare in un sistema una volta completata la progettazione anziché essere parte integrante del processo di progettazione.
2. Molti utenti e perfino gli amministratori della sicurezza vedono una forte sicurezza come un ostacolo al funzionamento efficiente e facile da usare di un sistema informativo o all’utilizzo delle informazioni.

**Nomenclatura**

**Attacco alla sicurezza**: qualsiasi azione che comprometta la sicurezza delle informazioni possedute da un'organizzazione.

**Meccanismo di sicurezza**: un processo (o un dispositivo che incorpora tale processo) progettato per rilevare, prevenire o recuperare da un attacco alla sicurezza.

**Servizio di sicurezza**: un servizio di elaborazione o comunicazione che migliora la sicurezza dei sistemi di elaborazione dei dati e i trasferimenti di informazioni di un'organizzazione. I servizi hanno lo scopo di contrastare gli attacchi alla sicurezza. Fanno uso di uno o più meccanismi di sicurezza.

**Minaccia**: qualsiasi circostanza o evento con il potenziale di avere un impatto negativo sulle operazioni organizzative, sui beni organizzativi, sugli individui, su altre organizzazioni o sulla Nazione, inclusa missione, funzioni, immagine o reputazione. Attraverso un sistema informativo mediante accesso non autorizzato, distruzione, divulgazione, modifica delle informazioni e/o negazione del servizio.

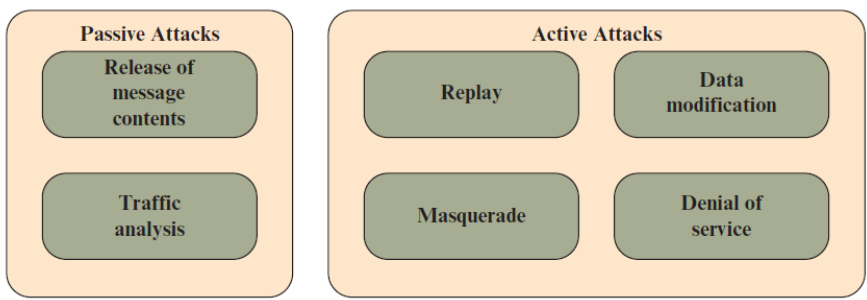
**Attacco**: qualsiasi tipo di attività dannosa che tenta di raccogliere, interrompere, negare, degradare o distruggere le risorse del sistema informativo o le informazioni stesse.

**Attacchi alla sicurezza**

Un mezzo utile per classificare gli attacchi alla sicurezza è in termini di attacchi passivi e attacchi attivi.

Un attacco passivo tenta di apprendere o utilizzare informazioni dal sistema ma non influisce sulle risorse del sistema.

Un attacco attivo tenta di alterare le risorse di sistema o di influenzarne il funzionamento.



**Attacchi passivi**

Gli attacchi passivi consistono nell'intercettare o nel monitorare le trasmissioni.

L'obiettivo dell'aggressore è ottenere le informazioni che vengono trasmesse.

Gli attacchi passivi sono molto difficili da rilevare perché non comportano alcuna alterazione dei dati.

In genere, il traffico dei messaggi viene inviato e ricevuto in modo apparentemente normale e né il mittente né il destinatario sono consapevoli che una terza parte ha letto i messaggi o osservato lo schema del traffico.

Tuttavia è possibile impedire il successo di questi attacchi, nella maggior parte dei casi mediante la crittografia.

Pertanto, l’enfasi nella gestione degli attacchi passivi è posta sulla prevenzione piuttosto che sul rilevamento.

Il rilascio del contenuto del messaggio è facilmente comprensibile. Vorremmo evitare che un avversario venga a conoscenza del contenuto di queste trasmissioni.

L’analisi del traffico è più sottile:

* Supponiamo di avere un modo per mascherare il traffico di informazioni in modo che gli avversari non possano estrarre le informazioni dal messaggio. La tecnica comune per mascherare i contenuti è la crittografia.
* Se avessimo adottato una protezione crittografica, un avversario potrebbe comunque essere in grado di osservare lo schema di questi messaggi.
* L'avversario potrebbe determinare la posizione e l'identità degli host comunicanti e potrebbe osservare la frequenza e la lunghezza dei messaggi scambiati.
* Questa informazione potrebbe essere utile per indovinare la natura della comunicazione che stava avvenendo.

**Attacchi attivi**

Gli attacchi attivi comportano la modifica del flusso di dati o la creazione di un flusso falso e può essere suddiviso in quattro categorie:

* replay
* mascheramento
* modifica dei messaggi
* denial of service

Gli attacchi attivi presentano le caratteristiche opposte degli attacchi passivi.

Sebbene gli attacchi passivi siano difficili da individuare, esistono misure per prevenirne il successo

Sebbene gli attacchi passivi siano difficili da individuare, esistono misure per prevenirne il successo. D’altro canto, è piuttosto difficile prevenire in modo assoluto gli attacchi attivi, perché per farlo sarebbe necessaria la protezione fisica di tutti i mezzi e le vie di comunicazione in ogni momento.

L’obiettivo è individuarli e riprendersi da eventuali interruzioni o ritardi da essi causati.

Poiché il rilevamento ha un effetto deterrente, può anche contribuire alla prevenzione.

Il **replay** comporta l'acquisizione passiva di un'unità di dati e la sua successiva ritrasmissione per produrre un effetto non autorizzato.

Gli attacchi di replay consistono nella cattura di tipo passivo di porzioni di traffico e nel tentativo successivo di reiniettare il traffico catturato all’interno della rete in modo da avere un effetto non autorizzato.

Non necessariamente implica che l’attaccante conosca esattamente il contenuto del traffico che sta reiniettando.

La **modifica dei dati** significa semplicemente che una parte di un messaggio legittimo viene alterata o che i messaggi vengono ritardati o riordinati per produrre un effetto non autorizzato. Ad esempio, un messaggio che dice "Consenti a John Smith di leggere gli account di file riservati" viene modificato in "Consenti a Fred Brown di leggere gli account di file riservati".

Fine 18/10

Un **masquerade** ha luogo quando un'entità finge di essere un'entità diversa. Un attacco mascherato di solito include una delle altre forme di attacco attivo. Ad esempio, le sequenze di autenticazione possono essere acquisite e riprodotte dopo che è stata eseguita una sequenza di autenticazione valida, consentendo così a un'entità autorizzata con pochi privilegi di ottenere privilegi aggiuntivi impersonando un'entità che dispone di tali privilegi.

Il **denial of service** impedisce o inibisce il normale utilizzo o gestione delle strutture di comunicazione. Questo attacco potrebbe avere un obiettivo specifico. Infatti, un'entità può sopprimere tutti i messaggi diretti a una particolare destinazione (ad esempio, il servizio di controllo della sicurezza).

Un'altra forma di denial of service è l'interruzione di un'intera rete (**denial of network service**), sia disabilitando la rete sia sovraccaricandola di messaggi in modo da peggiorare le prestazioni.

24/10

**Recap**

Abbiamo visto una prima classificazione degli attacchi informatici: questi attacchi possono essere classificati come passivi o attivi.

Gli attacchi passivi sono quelli che non implicano un’azione attiva (l’invio o la modifica di qualsiasi tipo del traffico) da parte dell’attaccante. Proprio per questo sono molto difficili da rilevare in quanto non lasciano traccia e l’unica cosa da fare è adattare delle configurazioni che li prevengano, o comunque delle azioni che impediscano ad un attacco di tipo passivo di andare a buon fine, di essere efficace.

Al contrario, gli attacchi attivi sono quelli che prevedono o l’invio di traffico oppure la modifica di qualsiasi tipo del traffico da parte di un attaccante. La cosa più fattibile è la rilevazione tempestiva dell’attacco (prima che l’attacco abbia portato a problemi seri all’interno della rete o del sistema), mentre una prevenzione a priori è praticamente impossibile perché le sfide a cui sono sottoposti gli attaccanti e chi progetta sistemi di sicurezza sono opposte. L’attaccante deve trovare una falla per portare a termine il suo attacco, chi progetta il sistema di sicurezza deve tappare tutte le falde esistenti e deve prevedere in anticipo eventuali possibili security hall, quindi buchi di sicurezza che permettono di effettuare un attacco a cui ancora nessuno ha pensato. Siccome i modi di pensare associati a eseguire l’attacco e alla difesa sono diversi è molto difficile a priori cercare di prevenire qualsiasi tipo di attacco.

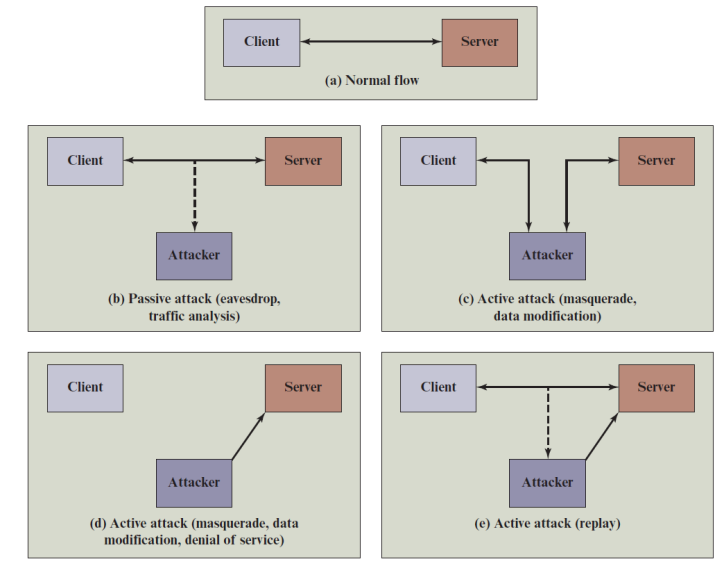
Per gli attacchi passivi la cosa è più ragionevole è la prevenzione, mentre per gli attacchi attivi la cosa più ragionevole è rilevazione tempestiva e poi la rilevazione di recupero, ovvero rilevare l’attacco e bloccarlo prima che abbia fatto danni significativi.

Nella realtà gli attacchi, soprattutto quelli più complessi, avranno sia una componente attiva sia una passiva. Saranno quindi inizialmente preceduti da una fase passiva di osservazione del traffico e di acquisizione delle informazioni che poi servono per effettuare la parte attiva dell’attacco.

I quattro macrotipi di attacco sono: replay (attacco di rilancio), di mascheramento (o impersonificazione), modifica dei messaggi e impedimento del servizio.

In realtà è molto difficile andare a categorizzare un attacco esclusivamente all’interno di questi 4, tipicamente è una combinazione di questi.

**Attacchi alla sicurezza**



Nello schema (a) è rappresentato il flusso normale del traffico, quindi da un client a un server, assumendo che la maggior parte delle applicazioni che sono in rete obbediscono al paradigma client-server.

Negli attacchi passivi (b) la linea tratteggiata significa che l’attaccante acquisisce informazioni in maniera passiva, mentre la linea continua significa scambio di traffico vero e proprio. Quindi negli attacchi passivi, sia quelli di ascolto sia quelli di analisi del traffico, l’attaccante acquisisce il traffico senza farsi scoprire, in maniera passiva e senza modificarlo.

Nell’attacco attivo (e) di replicazione l’attaccante acquisisce del traffico, che può essere anche cifrato, e l’attaccante non necessariamente riesce a decodificare il traffico cifrato, può anche prendere il traffico cifrato così com’è e poi lo reinietta in rete. In questo esempio c’è client-server ma possiamo vederlo tipicamente come la rete a cui è attaccato il server. Questo perché sappiamo che gli effetti degli attacchi possono essere sia sulla rete sia sui sistemi terminali, non necessariamente sui sistemi terminali. La cybersecurity considera sia la sicurezza delle informazioni sia la sicurezza di rete perché le cose sono legate. Posso impedire ad esempio di accedere alle informazioni semplicemente bloccando il servizio di rete, senza andare a bloccare il sistema terminale. A seconda della configurazione del sistema terminale o della rete a cui il sistema terminale è attaccato reiniettare questo traffico può dar origine ad effetti indesiderati.

Effetti indesiderati: se il traffico fosse potenzialmente legittimo potrebbe dar luogo a delle risposte, se la rete invece è adeguatamente protetta è solo traffico di disturbo.

La prima misura per controbattere gli attacchi di replay è utilizzare i numeri di sequenza. Se catturo un pacchetto che ha un numero di sequenza e lo rilancio, il sistema terminale si accorge che quello è un pacchetto replicato. Se non lo posso modificare perché se lo vado a modificare ad esempio altero i campi che mi proteggono dalla modifica indesiderata dei pacchetti, il pacchetto non sarà più valido. Quindi se lo prendo così com’è e lo rilancio, un sistema terminale potrebbe riuscire ad accorgersi della modifica, poi dipende da dove viene fatta questa modifica.

In alcuni casi è possibile effettuare questa operazione senza problemi, ad esempio, se reinoltro porzioni di traffico udp, se non è implementato un meccanismo con un numero do sequenza a livello applicativo, il destinatario ogni volta risponderà alla stessa richiesta. Perché udp è un protocollo a datagramma, quindi non ha il concetto di sessione e non usa i numeri di sequenza e quindi tutte le applicazioni che usano udp sono potenzialmente sensibili ad attacchi di questo tipo a meno che non è l’applicazione stessa che usa i numeri di sequenza. È vero che abbiamo l’id del datagramma all’interno del protocollo ip che distingue tutti i datagrammi, però nessun router tiene memoria dei datagrammi già ricevuti. Quindi se invio un datagramma il router continuerà a inviarlo verso la destinazione. L’id del datagramma serve principalmente a gestire opportunamente le operazioni di frammentazione e riassemblaggio a destinazione.

Attacco di mascheramento o data modification o denial of service (d): l’attaccante invia del traffico. Non c’è l’attacco di replay perché non viene replicato nessun traffico precedentemente scambiato.

Gli attacchi di mascheramento o impersonificazione sono tutti gli attacchi in cui l’attaccante fa finta di essere un altro. In questo caso l’attaccante fa finta di essere un nuovo peer che sta inviando traffico in rete. Ad esempio, l’attaccante potrebbe utilizzare la tecnica dell’ip spoofing, quindi utilizzare un indirizzo ip diverso dal suo in modo tale che le risposte non arrivino a lui. È il classico attacco di denial of service.

Come faccio ad attaccare il mio client?

Consideriamo questo scenario:

Immagine che contiene testo, linea, diagramma, schermata

Descrizione generata automaticamente

L’attaccante può andare direttamente ad attaccare il client, ma magari sistemi di intrusion detection o intrusion protection del client potrebbero accorgersene.

La cosa più sicura è utilizzare del traffico originato da server legittimi.

Supponiamo che questo sia un server DNS ad alta capacità, cioè opportunamente ridondato per gestire grandi moli di traffico.

L’attante invierà del traffico, ad esempio una richiesta DNS (trasportata da udp) in cui l’ip della sorgente è IP\_c e l’ip della destinazione è IP\_s. L’attaccante sta impersonificando il client perché in questo modo, se il pacchetto riesce ad arrivare al server DNS, innescherà una risposta con IP\_SRC = IP\_s e IP\_DST = IP\_c.

Se effettuo questo attacco verso un numero molto elevato di server, ogni server vedrà una quantità di traffico modesta e quindi non si accorgerà, non avrà grossi problemi, e poi, se è un server DNS non risolverò sempre la stessa query ma potrei risolvere tutta una serie di siti well known, per cui so che quel DNS avrà la risposta pronta. Quindi mando la richiesta e ho la risposta. I server DNS si comporteranno come una batteria di attacchi di rilancio.

Di quanti attaccanti ho bisogno? Di uno solo, perché invierà a tutti questi server query di tipo DNS impersonificando (attacco di mascheramento) il client.

Il client è la nostra vittima, il traffico che gli arriverà sarà impegnativo e si troverà a dover gestire tutta una serie di risposte che sono del tutto legittime.

Come si blocca un attacco di questo tipo?

Supponendo che in mezzo ci sia un sistema di protezione, il firewall (FW), dovremo implementare una codifica che impedisca a delle risposte a cui non corrispondono precedenti richieste di attraversare il nostro muro. Questa è una prima cosa.

L’altra cosa che si può fare è prevenire che la propria rete sia utilizzata da un attaccante per fare operazioni di questo tipo. Si può limitare il numero delle reti che possono partecipare in maniera inconsapevole a un attacco di questo tipo.

Sarebbe opportuno configurare anche il firewall presente verso il client con opportune codifiche di ingresso, ovvero se il traffico di uscita ha un indirizzo ip che non è compatibile con le reti interne, il traffico non va inoltrato perché significa che c’è qualcosa che non va. Il messaggio viene scartato in maniera silente senza generare messaggi ICMP altrimenti l’obiettivo è proprio quello di inondare la rete con messaggi ICMP.

Queste due politiche si applicano solo a reti terminali. Esempio:

Immagine che contiene diagramma, calligrafia, disegno, Line art

Descrizione generata automaticamente

L’operazione da fare sul client vale per tutti quei sistemi che offrono dei servizi, perché se un sistema non offre dei servizi ci sarà già un firewall che permette il transito di pacchetti solo da dentro verso fuori, e non da fuori verso dentro.

Su un sistema di transito le cose sono più complicate: in questo caso la rete è configurata per trasportare traffico, e quindi è complesso decidere se del traffico è legittimo o meno.

Questo invece è un altro classico attacco di mascheramento o di man in the middle. L’attaccante cerca di impersonificare il client verso il server e di impersonare il server verso il client: in questo modo impedisce che ci sia un colloquio diretto tra i due e può aggiungere, cancellare o modificare il traffico, tutto questo come attacco di data modification (c). questi sono tanto più efficaci se non c’è il canale diretto, cioè se il canale originale viene bloccato e si obbliga il traffico a passare attraverso una terza parte. Contromisure: sono tutte quelle atte a rilevare la modifica dei dati e quindi tutte le tecniche che rientrano sotto l’obiettivo di data integrity o message integrity. Applico un hash crittografico per garantire l’integrità del messaggio. Prendo un pacchetto, calcolo l’hash, che è una funzione unidirezionale che per input di dimensioni variabili da sempre un output di dimensione fissa: il digest. Poi il digest lo cifro con la chiave privata del mittente, in modo tale che a destinazione le operazioni che vanno fatte per capire se il pacchetto è stato modificato sono le seguenti. Prendo il pacchetto in chiaro, prendo il digest, conosco tutti gli algoritmi, calcolo il digest. Quindi prendo il contenuto del pacchetto, lo passo alla funzione di hash e genero l’hash. Poi prendo l’hash crittografico cifrato con la chiave privata e lo decifro con la chiave pubblica del mittente. E controllo se l’hash che ho ottenuto dal payload del pacchetto è uguale all’hash crittografico. Se sono uguali significa che nessun bit è stato modificato.

La soluzione tipica di questo problema del man in the middle è utilizzare una terza parte che si chiama entità o autorità di certificazione, che non fa altro che andare a firmare la chiave pubblica del client. Questo perché l’attaccante può usare la sua chiave pubblica e andare a modificare i dati. Se invece il client e il server hanno una chiave pubblica firmata da un’autorità di certificazione, di cui è nota all’interno dei calcolatori già dentro al sistema operativo la loro chiave pubblica, allora in quel caso, se ci si fida dell’autorità di certificazione automaticamente ci si fida anche di quelli di cui l’autorità di certificazione fa da garante.

La strategia per evitare la modifica dei dati è quella di utilizzare degli hash crittografici e delle firme digitali. Questo vale sia per il traffico sia per i dati.

(Esempio: Certificato X.509, è la chiave pubblica firmata)

Nel caso di data modification le cose cambiano a seconda del tipo di protocollo che andate ad utilizzare e si possono avere garanzie più o meno forti. Se si ha un protocollo basato sul concetto di sessione è possibile andare a proteggere l’intera sessione, oppure i dati, oppure il singolo messaggio. Se invece avete un protocollo a datagramma, cioè udp, è possibile solo inserire i meccanismi di data integrity direttamente nell’applicazione e quindi si può proteggere solo il singolo messaggio, niente di più.

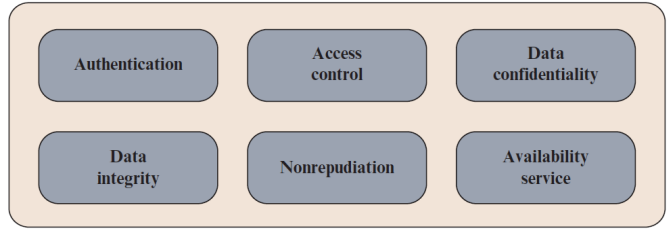
**Servizi di sicurezza**

Per proteggermi dagli attacchi devo mettere in piedi un certo numero di servizi di sicurezza.

Un servizio di sicurezza cerca di soddisfare i requisiti di uno o più dei 5 obiettivi della sicurezza: confidenzialità, integrità, disponibilità, autenticità e accountability (CIA + AA).

I servizi di sicurezza (che sono quelli nel disegno: servizio di autenticazione, di controllo dell’accesso, confidenzialità dei dati, integrità dei dati, non ripudiabilità e servizi di disponibilità):

* implementano delle politiche di sicurezza, il cui compito è quello di soddisfare i requisiti dei nostri obiettivi;
* sono implementati da meccanismi di sicurezza.



Questi servizi, combinati, di solito non vanno mai da soli, hanno l’obiettivo di soddisfare i requisiti degli obiettivi di sicurezza.

**A final recap**

Immagine che contiene testo, schermata, linea, diagramma

Descrizione generata automaticamente

Gli obiettivi di cybersecurity principali (confidenzialità, integrità, disponibilità, autenticità e accountability) danno luogo a un certo numero di requisiti e definiscono anche cosa si intende per perdite di sicurezza, ovvero quando i requisiti non sono soddisfatti.

Questi obiettivi li implementiamo attraverso le politiche di sicurezza. Le politiche di sicurezza vengono implementate attraverso i security service, che a loro volta sfruttano un certo numero di meccanismi di sicurezza.

Nell’implementazione dobbiamo fronteggiare un certo numero di sfide: ne abbiamo viste 10 ma possiamo classificarle sotto queste tre macrocategorie:

* gli attacchi (attivi o passivi)
* i criteri di usabilità (e in generale di disponibilità degli utenti ad accettare meccanismi di sicurezza). Questo perché sappiamo che in alcuni casi sono gli utenti che mal digeriscono delle politiche di sicurezza restrittive, in altri casi sono gli stessi operatori di rete che fino a quando non subiscono un danno significativo tendono a sottostimare l’importanza della sicurezza all’interno dei propri servizi o delle proprie reti oppure sono essi stessi che lo ritengono come ostativo all’utilizzabilità dei servizi stessi
* motivi di tipo economici, CAPEX e OPEX (CAPEX: capital expenditure, OPEX: operational expenditure).

**Approfondimento su CAPEX e OPEX**

I CAPEX sono gli investimenti, cioè i soldi che si investono per dotare l’azienda di un nuovo prodotto o servizio. L’OPEX sono i soldi che bisogna investire per mantenerlo funzionante. Nel CAPEX, che di solito si fa una volta sola, ci sono tutti quei costi sono richiesti per mettere in opera il servizio, mentre nell’OPEX per mantenerlo funzionante. Per mettere in opera il servizio bisogna ad esempio acquistare i dispositivi e/o fare training al personale o assumere personale che li sappia usare. Oppure utilizzare soluzioni open source o proprietarie sui dispositivi che si hanno già e formare delle persone già vostre per saperle utilizzare. Questa formazione può avere un costo esplicito (si fa un corso da qualche parte) o implicito (parte delle ore del lavoro di quelle persone saranno demandate alla formazione).

L’OPEX è quanto mi costa mantenere in piedi il servizio, cioè la formazione permanente del personale (corsi di aggiornamento che possono essere fisici, online) ed eventuali aggiornamenti del software.

Sono concetti generalissimi che valgono per qualsiasi sistema o servizio, ma sono concetti importanti: ogni volta che viene fatto un investimento bisogna capire quanto costa all’inizio e quanto costa mantenerlo. Soprattutto quello che in alcuni casi viene sottostimato è l’OPEX.

Anche per quanto riguarda la sicurezza è importante il CAPEX ma è importante soprattutto l’OPEX. Se metto in piedi un sistema di sicurezza e poi non lo aggiorno più, il sistema di sicurezza diventerà obsoleto e sarà come non averlo, o anzi offrirà delle vulnerabilità note a potenziali attaccanti, proprio perché non mi sono preoccupato di andare ad aggiornarlo quando venivano rilasciati gli aggiornamenti che andavano a riparare le falle su vulnerabilità note che precedentemente non erano ancora conosciute.

**Autenticazione e controllo degli accessi**

I servizi di sicurezza di autenticazione e controllo degli accessi spesso vanno insieme.

L’autenticazione permette di accedere a un servizio solo dopo che ci conosce l’identità di chi vuole accedere. Permette quindi la comunicazione solo quando l’identità è nota, dove l’identità può essere sia di un utente umano, sia di una macchina. Questo implica che i due comunicanti devono utilizzare un protocollo comune per comunicare.

Il servizio di autenticazione tipicamente serve a evitare il problema del man in the middle, oppure dell’intervento di una terza parte. Quindi se ho un servizio di autenticazione, che mi permette di capire qual è l’identità del mio client, dovrei riuscire a prevenire gli attacchi di mascheramento.

Il **servizio di autenticazione** si occupa di garantire che una comunicazione sia autentica.

* Autenticazione di mittente/entità: garantire l'identità dei pari in una comunicazione (i peer utilizzano lo stesso protocollo per comunicare)
* Nessuna interferenza da parte di terzi mascherati

Il **controllo degli accessi** è la capacità di limitare e controllare l'accesso ai sistemi host e alle applicazioni tramite la rete. Potrebbe richiedere un'autenticazione preventiva.

Il controllo di accesso serve a limitare i diritti di accesso a un determinato sistema o servizio.

Di solito va con l’autenticazione, ma non è detto.

Bisogna discriminare tra un controllo dell’acceso interno o esterno. Se controllo l’accesso della rete dall’esterno verso l’interno utilizzerò tecniche di autenticazione e poi tecniche di controllo di accesso. Quindi alcuni utenti avranno accesso a determinati servizi, altri utenti avranno accesso ad altri servizi (diversi dai precedenti), oppure posso utilizzare delle tecniche che non prevedono il controllo di accesso, ad esempio le VLAN. In questo caso, se sono all’interno della mia rete posso ad esempio impedire che i dipendenti dell’area amministrativa accedono ai server dove vengono caricati i progetti in via di sviluppo. Quindi effettuo il controllo dell’accesso mettendo delle limitazioni all’interno della rete, quindi “segregando” il traffico.

**Confidenzialità dei dati**

La confidenzialità dei dati è la protezione dei dati trasmessi da attacchi passivi (cioè l’ascolto per decodificare i contenuti).

Sono disponibili diversi livelli di protezione:

* Tutti i dati entrano/escono da un host
* Protezione della singola sessione
* Protezione del messaggio singolo

È differente a seconda dei protocolli che vengono utilizzati. Se utilizzo protocolli orientati alla sessione (tcp) posso proteggere il socket aperto dal tcp a livello di sessione, oppure a livello di messaggio (questo posso farlo anche con udp, ma inserendo la confidenzialità dei dati dentro l’applicazione), oppure posso proteggere tutti i dati che entrano ed escono da un sistema.

Protezione dall'analisi del traffico: sposto la cifratura, quindi mi proteggo tramite l’offuscamento. Devo cifrare il più possibile all’interno del traffico. Se riesco a cifrare non solo lo strato applicativo, ma anche lo strato 3 e 4, un utente malintenzionato non sarà in grado di osservare gli indirizzi ip mittente e destinazione, le porte, e quindi complico parecchio il lavoro dell’attaccante.

Per fare questo devo fare la cifratura a strato 2, cosa che ad esempio viene sempre fatta nelle reti wireless, che però hanno altri problemi.

Un’altra vulnerabilità tipica del traffico che viene esposta attraverso le tecniche di analisi del traffico è quella di andare a stimare la dimensione dei messaggi e la loro frequenza: potrei fare anche questo andando ad alterare la dimensione dei messaggi. Questo di solito si fa con un meccanismo di sicurezza chiamato padding, che inserisce byte inutili alla fine del messaggio che servono a variare in maniera artificiale il numero dei byte all’interno dei pacchetti. Oppure potrei anche inviare dei pacchetti vuoti, solo per mascherare l’attività dei client.

Se non riesco a risalire all’identità di chi sta scambiando le informazioni perché sto cifrando anche lo strato 3 e lo strato 4, o con tecniche di cifratura allo strato 2 per le reti wireless, o con tecniche di vpn allo strato 3, e poi vado ad alterare la dimensione dei pacchetti o inserisco pacchetti artificiali che non hanno informazione, allora vado a complicare in maniera significativa il compito di chi va ad effettuare traffic analysis, andando ad offuscare le statistiche del traffico.

Questo non crea problemi a chi effettua monitoring legittimo del traffico, che ha accesso al pacchetto originale e quindi sarà in grado di discriminare qual è il traffico corretto e quale invece serve solo come offuscamento.

**Integrità dei dati**

Si utilizzano tipicamente meccanismi a chiave asimmetrica (chiave pubblica e chiave privata). Esistono anche meccanismi chiamati keyless, cioè senza chiave, basati sull’utilizzo di numeri pseudo casuali, ma sono meno utilizzati.

Nel caso di protocolli orientati alla sessione riesco a fornire protezione non solo sulla modifica dei dati ma anche ad esempio sulla loro cancellazione o sulla loro duplicazione, proprio perché utilizzo i numeri di sequenza e quindi mi accorgo se un dato mancava all’interno della sessione oppure se un dato è stato duplicato.

Se invece ho un meccanismo non orientato alla sessione, quindi orientato esclusivamente al datagramma, posso solo andare a stimare se il messaggio che ho ricevuto è integro oppure no, senza nessun legame con i messaggi precedenti.

L'integrità può applicarsi a un flusso di messaggi, a un singolo messaggio, a campi selezionati all'interno di un messaggio.

Un servizio di integrità orientato alla connessione garantisce che i messaggi vengano ricevuti così come inviati senza duplicazioni, inserimenti, modifiche, riordini o ripetizioni.

Questo servizio copre anche la distruzione dei dati.

Il servizio di integrità orientato alla connessione affronta sia la modifica del flusso di messaggi che la negazione del servizio.

Un servizio di integrità senza connessione generalmente fornisce protezione solo contro la modifica dei messaggi.

Tutti i servizi di integrità possono prevedere il recupero oppure no.

**Non ripudiabilità e disponibilità**

La **non ripudiabilità** impedisce al mittente o al destinatario di negare un messaggio trasmesso o ricevuto.

Come si attua questo servizio? Con il meccanismo della notarizzazione, quindi con una terza parte trusted, fidata, a cui sia il mittente che il destinatario si rivolgono per essere sicuri che il destinatario non dica di non aver ricevuto il messaggio e il mittente non dica di non averlo spedito.

Il notaio, che in genere fa capo alla presenza di un’autorità di certificazione, fa sì che se mi è arrivato un messaggio firmato con il certificato del client, il client non può dire che non l’ha inviato, e così per il server.

La **disponibilità** è la proprietà di un sistema di essere accessibile e utilizzabile su richiesta da un'entità di sistema autorizzata.

Come si realizza questo servizio? Con l’autenticazione e controllo di accesso. Se limito l’accesso a un determinato numero di utenti, tipicamente rendo un servizio disponibile.

Posso farlo sia per gestire sovraccarichi del traffico, sia per gestire attacchi informatici.

Problema tipico che si verifica in alcuni eventi imprevisti: ad esempio quando c’è stato l’attentato alle torri gemelle sono andati giù tutti i server DNS che stavano nei seminterrati e quindi il traffico internet è stato rallentato perché tutto il traffico gestito da quei server è stato dirottato su altri server, quindi, c’è stato un calo delle prestazioni. In quel caso c’è stato un problema di indisponibilità.

Quindi in alcuni casi la potenza di disponibilità può dipendere da una cattiva progettazione, in altri da un evento inaspettato e in altri da attacchi di cybersecurity.

Altri richiedono un'azione fisica per prevenire/ripristinare la perdita di disponibilità di elementi di un sistema distribuito.

**Meccanismi di sicurezza**

Immagine che contiene testo, schermata, Carattere, numero

Descrizione generata automaticamente

I meccanismi crittografici sono alla base del servizio di confidenzialità.

I meccanismi che assicurano l’integrità dei dati sono alla base del servizio di data integrity, insieme a quelli di firma digitale.

I protocolli di autenticazione che sono alla base del servizio di autenticazione.

Il padding che è alla base del servizio di prevenzione e analisi del traffico.

I meccanismi di routing control e di access control che possono permettere di mitigare problemi di disponibilità. Ad esempio, se ho una piattaforma che sta andando in sovraccarico mettere in piedi un meccanismo che permetta di replicare il servizio da un’altra parte e di dirottare efficacemente il servizio da un’altra parte è un meccanismo efficace per mitigare problemi di disponibilità.

La notarizzazione è il meccanismo abilitante dei servizi di non ripudiabilità.

**Tipi di sicurezza di rete**

La cybersecurity la possiamo classificare sotto due grandi topologie: la sicurezza dell’informazione e la sicurezza della rete.

A sua volta la sicurezza della rete possiamo classificarla come la sicurezza della comunicazione, che tipicamente implemento attraverso la combinazione di protocolli e tecniche crittografiche, e la sicurezza dei dispositivi. Sono tutte tecniche che ricadono nella protezione dei dispositivi, o dei sistemi terminali, o delle reti che permettono a quei sistemi di accedere a Internet.

* Sicurezza delle comunicazioni: viene implementata con l’uso combinato di un certo numero di protocolli, a vari livelli protocollari, dipende dal tipo di sicurezza che voglio implementare, che andranno combinati con tecniche di sicurezza, che possono essere sicurezza simmetrica, asimmetrica o key-less.
* Sicurezza dei dispositivi (o di insiemi di dispositivi): protezione dei dispositivi di rete e dei sistemi terminali collegati alla rete. Avremo meccanismi che regolano l’accesso (firewall), meccanismi che rilevano le intrusioni e meccanismi che prevengono le intrusioni.

Un meccanismo di prevenzione delle intrusioni è configurato per rilevare e bloccare un certo numero di intrusioni note.

Un meccanismo per la rilevazione delle intrusioni è un meccanismo che può essere configurato per rilevare intrusioni note o anche per rilevare attacchi 0-day.

Un IPS tipicamente non può essere utilizzato per gli attacchi 0-day.

Immagine che contiene testo, schermata

Descrizione generata automaticamente

**Sicurezza nello stack del protocollo IP**

Immagine che contiene testo, schermata, Carattere, linea

Descrizione generata automaticamente

I protocolli li posso applicare allo strato 3: IPSec, tra lo strato 4 e lo strato applicativo, quindi a livello di socket, oppure allo strato applicativo: riesco a proteggere anche il protocollo UDP, oppure a livello di strato 2.

Immagine che contiene testo, calligrafia, linea, Carattere

Descrizione generata automaticamente

Se li applico allo strato 2 hanno effetto non da estremo a estremo, no su grandi porzioni di rete, ma solo sul collegamento di questa tecnologia specifica. Quando cambio collegamento devo ripetere tutta l’operazione.

Le tecniche a strato 3 (tecniche tipicamente di VPN) avranno effetto solo su porzioni della rete, quelle coperte dal servizio VPN, quindi punto di ingresso e punto di uscita della VPN. Sono tecniche sopra TCP e quindi avranno effetto da estremo a estremo, quindi da client a server o da client a proxy (se ho una middlebox).

Application level sono veramente da estremo a estremo.

Nel mondo cloud esistono poi altri protocolli che servono per interconnettere i sistemi terminali che emulano alcune di queste tecnologie.

**Tipologie di minacce a livello applicativo**

Immagine che contiene testo, schermata, numero, Carattere

Descrizione generata automaticamente

**Implementazione delle politiche di sicurezza**

**Immagine che contiene testo, linea, diagramma, Carattere

Descrizione generata automaticamente**

Nel caso della sicurezza delle reti abbiamo la sicurezza della comunicazione, che la realizzo tramite l’uso congiunto di protocolli e tecniche crittografiche.

Nel caso della sicurezza dei dispositivi o di insiemi di dispositivi avrò dispositivi di controllo e dispositivi di rilevazione e prevenzione delle minacce.