appunti

Attenti alle reti

La telematica si basa prevalentemente sulle reti come mezzo di comunicazione per cui è indispensabile adottare strategie di sicurezza per difendere i sistemi di supervisione remoti da eventuali attacchi informatici

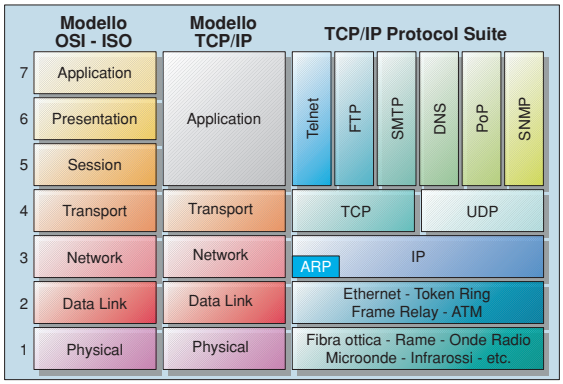
DANIELE CATTANEO

La rete è una componente fondamentale della telematica; se da un lato Internet agevola la diffusione dei sistemi di controllo remoti dall'altro presenta problematiche legate alla sicurezza di rete distinte tra sicurezza dei sistemi informativi e dei singoli calcolatori. Anche nei sistemi di controllo remoti è decisivo affrontare l'aspetto 'sicurezza di rete'; cosa accadrebbe, infatti, se in un processo di supervisione remoto fossero modificate abusivamente le variabili di gestione di un impianto industriale? Le conseguenze potrebbero anche essere catastrofiche.

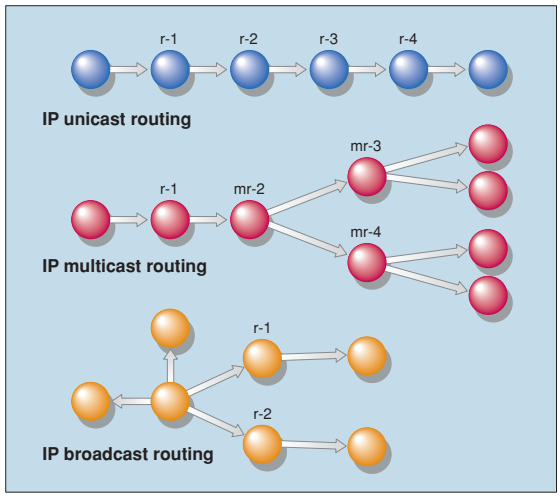
Rete e attacchi informatici

La sicurezza di rete è un tema che richiede particolare attenzione nella progettazione e gestione di un sistema di controllo remoto, come accennato. Gli attacchi alla sicurezza di rete, in particolare, sono classificabili in minacce passive se realizzate con intercettazioni (tentativi da parte di terzi di accedere alle informazioni trasmesse all'interno della rete) e in minacce attive se l'accesso alle informazioni trasmesse da parte di un'entità non autorizzata è seguito dall'alterazione delle stesse informazioni in modo che arrivino al sistema destinatario manipolate e con valori falsi.

Da questo concetto si intuisce allora come le tecniche di protezione possano coinvolgere l'architettura di rete: solo conoscendo bene le caratteristiche dell'architettura di rete e le modalità con cui la rete può essere attaccata è possibile progettare sistemi di sicurezza ad hoc.



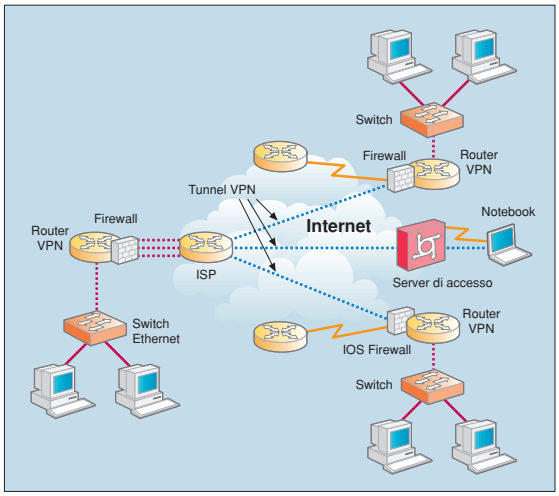
Modello ISO OSI e corrispondenze con i protocolli utilizzati nella rete Internet



Il firewall deve rifiutare i pacchetti destinati a un indirizzo di tipo broadcast e i pacchetti il cui indirizzo origine sia di tipo multicast o broadcast

Internet e protocolli TCP/IP

I sistemi di controllo utilizzano spesso servizi web per interfacciarsi alla rete Internet per cui la rete interna diventa vulnerabile rispetto ad alcune tecniche di attacco che hanno come obiettivo la violazione o la distruzione di informazioni. Un servizio per essere definito 'sicuro' deve garantire sia il proprio utilizzo solo e soltanto per le operazioni previste sia l'impossibilità di intercettare e falsificare le transazioni che avvengono attraverso il servizio stesso. Per capire le tecniche di protezione di rete è necessario ripassare brevemente come sono composti i pac-



La rete VPN è più sicura perché i dati sono incapsulati (tunneling) attraverso i router quando viaggiano da un'origine a una destinazione

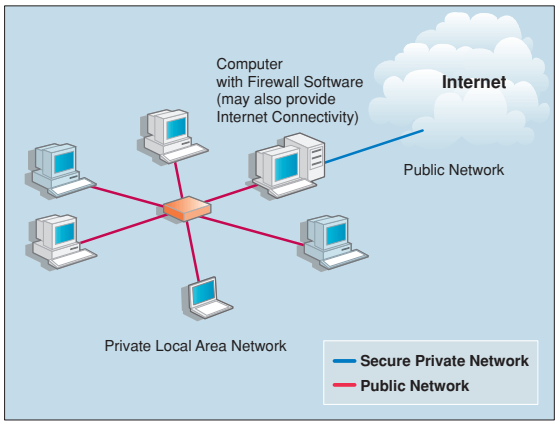
chetti in ciascuno strato software dell'architettura TCP/IP, il protocollo più diffuso nella rete Internet. Un pacchetto è composto a ogni livello da una testata (header, che contiene le informazioni rilevanti per il protocollo) e da dati (payload); la costruzione del pacchetto avviene livello per livello ovvero ciascuno strato aggiunge le proprie informazioni di controllo al campo dati ricevuto dallo strato superiore (tecnica nota con il nome di incapsulamento).

Protocollo IP

Al protocollo IP è delegato il servizio di Internetworking e il trasporto dei pacchetti è indipendente dalla rete fisica utilizzata, sia essa locale o geografica. I pacchetti sono di tipo 'unicast' se spediti verso un unico host destinatario, 'multicast' se spediti a un gruppo di host e broadcast se indirizzati a tutti gli host in grado di riceverli nell'ambito della rete logica di appartenenza. Il multicast serve soprattutto per migliorare l'efficienza di trasmissione: se più host richiedono la medesima informazione un pacchetto multicast consente la spedizione delle informazioni trasmettendo una sola copia del pacchetto invece di inviare a ogni host un pacchetto di tipo unicast. E' impor-

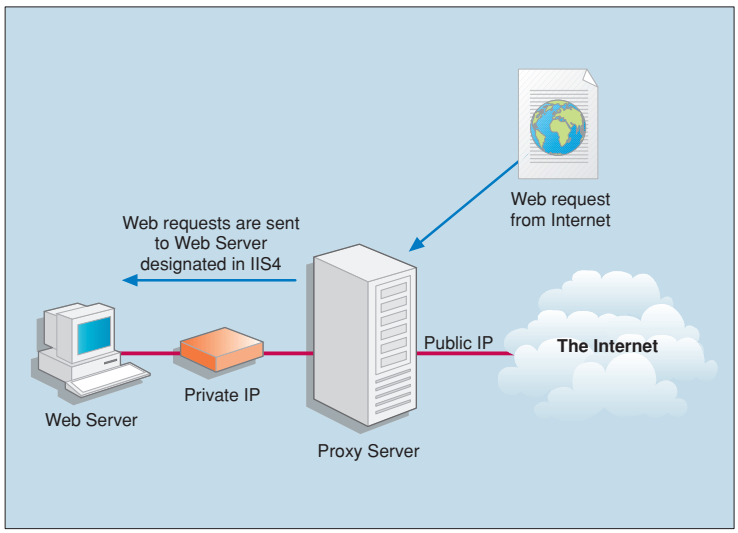
tante sottolineare che gli indirizzi di tipo broadcast e multicast sono indirizzi di destinazione non di origine; tali indirizzi, infatti, potrebbero essere utilizzati in un attacco informatico per utilizzare la macchina di destinazione e amplificare gli effetti dell'attacco. Un firewall, allora, deve innanzitutto rifiutare i pacchetti destinati a un indirizzo di tipo broadcast e i pacchetti il cui indirizzo origine sia di tipo multicast o broadcast. Ma il controllo non si limita a questi campi: il campo option nell'intestazione del pacchetto, infatti, è raramente utilizzato nel protocollo IP e può essere utilizzato per eventuali attacchi.

Gli insediamenti produttivi con supervisione remota necessitano di reti telematiche di assoluta sicurezza perché un attacco informatico potrebbe avere conseguenze catastrofiche



Il firewall impedisce gli accessi non autorizzati attraverso il controllo dell'accesso alle reti e l'intercettazione di tutti i messaggi in entrata e in uscita

L'opzione di 'source routing', per esempio, consente al mittente di specificare il percorso che il pacchetto dovrebbe seguire per giungere a destinazione (piuttosto che seguire il percorso indicato dai router attraverso la loro router table, una tabella particolare dove il router decide a quale altro router inviare il pacchetto). Questa opzione è nata per aggirare i router con routing table errata o non funzionante ma di fatto è utilizzata solo per attacchi che tentano di aggirare le misure di sicurezza con cammini non consueti. Un sistema di sicurezza, allora, può essere impostato in modo tale da scartare tutti i pacchetti che hanno le opzioni di testata valorizzate.
Nel protocollo IP un'altra tipologia di attacco può sfruttare le tecniche di frammentazione dei pacchetti: pacchetti di grandi dimensioni, infatti, sono frammentati in pacchetti di dimensioni minori perché supportati dalle reti fisiche attraversate. Solo il primo frammento contiene le informazioni relative al livello più alto quindi, dal punto di vista della sicurezza, questo pacchetto è controllato dai sistemi di firewall. Gli attaccanti possono nascondere delle informazioni nelle parti in cui i frammenti successivi si sovrappongono (accade solo nel caso di errori o di attacchi perché generalmente ogni frammento inizia dopo la fine del precedente); se per qualche ragione non è possibile riassemblare i pacchetti nel firewall è meglio scartare tutti i frammenti e perdere le informazioni ricevute, ed è certamente meno rischioso di un potenziale attacco.



Il proxy server permette di filtrare gli accessi ai servizi web con cui sono gestite le applicazioni di controllo remoto

Protocollo TCP

Il protocollo TCP è il livello di trasporto più diffuso in Internet e riguarda, solo per citare qualche esempio, i servizi http, smtp, ftp e telnet. Il protocollo TCP garantisce che la destinazione riceva i dati applicativi nello stesso ordine con cui sono stati inviati integralmente (tutti i dati sono stati ricevuti) e senza dati duplicati. La connessione a un host può essere chiusa se non sono garantite le tre proprietà descritte. A questo livello è effettuato il riconoscimento dei pacchetti di apertura e di chiusura di una connessione: questo è importante in termini di sicurezza perché consente ai client interni a una rete di connettersi ai server esterni alla rete e vietare ai client esterni alla rete di connettersi ai server interni. Gli attacchi sul protocollo TCP possono derivare, per esempio, dalla manipolazione dei numeri di sequenza con cui i pacchetti sono inviati con l'effetto di dirottare la connessione tra due host.

Valutare la sicurezza

Conoscendo l'architettura dei protocolli e le caratteristiche della rete utilizzata è necessario analizzare i rischi a cui si è esposti e procedere quindi con l'implementazione di strumenti e servizi per la protezione dell'informazione. In particolare l'analisi dei rischi può essere di tipo quantitativo, quando si valuta la probabilità che si verifichi un evento disastroso e le perdite stimate associate a tale evento, o di tipo qualitativo quando invece ci si concentra sull'individuazione delle risorse da proteggere, dei possibili attaccanti e delle possibili tecniche di attacco. Il secondo approccio è quello più diffuso. Dopo la valutazione dei rischi si considerano le strategie di difesa da parte di possibili attacchi alla rete. Una semplice strategia di sicurezza è quella conosciuta con il termine di 'security through obscurity' e presuppone che un sistema sia sicuro perché nessuno ne conosce l'esistenza. Purtroppo però è un approccio che non è efficace a lungo termine poiché nel momento di autenticazione a un server, per esempio, esiste uno scambio di informazioni sensibili con l'host per cui è possibile risalire anche all'hardware e al software del sistema operativo utilizzati.

Se la rete non è troppo articolata si può applicare la strategia di host security: ogni macchina ha un proprio sistema di sicurezza. La soluzione diviene complessa da gestire al crescere del numero di host perché sorgono problemi di scalabilità, sistemi operativi differenti, hardware con caratteristiche diverse, configurazioni eterogenee, ecc... La sicurezza a livello di host, inoltre, dipende fortemente dalle competenze di chiunque abbia un accesso privilegiato alla macchina.

E' sicuramente più vantaggiosa la tecnica di network security diffusa nelle grandi aziende e nelle reti di computer che adottano una strategia di rete. L'attenzione è focalizzata sul controllo agli accessi di rete e ai servizi offerti: un firewall protegge la rete e i sistemi interni mentre le procedure di autenticazione forte e la tecnica della cifratura consentono di proteggere dati particolarmente

Glossario

Cifratura o crittografia: tecnica di codifica dei messaggi testuali in simboli non interpretabili da chi non possiede la corretta chiave di lettura.

Client: PC o terminale collegato in rete che condivide servizi con altri PC.

Host: computer ospite. Accetta, tramite rete, le richieste di altri PC o terminali che possono così utilizzare programmi o condividere dati resi disponibili.

Pacchetto: gruppo di dati con un'intestazione (header).

Firewall: sistema che impedisce gli accessi non autorizzati attraverso il controllo dell'accesso alle reti e l'intercettazione di tutti i messaggi in entrata e in uscita.

Proxy Server: server con il compito di filtrare le informazioni che arrivano da Internet attraverso il firewall.

Router: dispositivo che sposta i dati tra segmenti di rete diversi in grado di leggere l'header del pacchetto di dati per determinare il percorso di trasmissione migliore. I router possono anche collegare segmenti di rete che utilizzano protocolli diversi tra loro.

Server: termine che indica un computer e un software che offrono servizi ai client quali memorizzazione dei file (file server), programmi (application server), condivisione di stampanti (print server), fax (fax server) o modem (modem server).

sensibili. Il least privilege è un principio fondamentale per la sicurezza e si basa sui privilegi minimi attribuiti a ogni categoria di utenti (amministratori, utenti generici, ecc...), programmi e sistemi: così non tutti gli utenti possono accedere a ogni servizio Internet o possono modificare o leggere file in un sistema. Il rischio, in questo caso, è l'errata valutazione di programmi e protocolli utilizzati in rete per cui viene impostato un numero di privilegi inferiore a quelli minimi.
Una combinazione di diverse tecniche di sicurezza è la strategia di 'defense in depth', ovvero si adottano meccanismi di network security, meccanismi di host security e meccanismi di sicurezza per gli utenti: si adottano strategie di configurazione per cui nel sistema è specificato solamente quanto è consentito vietando qualunque altra cosa (default deny) oppure, al contrario, si specifica solo ciò che è proibito abilitando qualunque altra cosa (default permit); dal punto di vista della sicurezza l'approccio preferibile è il default deny. ■