MARIO DI MAURO

Con allegato online

SICUREZZA NELLE COMUNICAZIONI SU RETE

Dai princìpi fondamentali ai paradigmi di nuova generazione, con esempi ed applicazioni pratiche

FrancoAngeli/Informatica

Informazioni per il lettore

Questo file PDF è una versione gratuita di sole 20 pagine ed è leggibile con

La versione completa dell'e-book (a pagamento) è leggibile con Adobe Digital Editions. Per tutte le informazioni sulle condizioni dei nostri e-book (con quali dispositivi leggerli e quali funzioni sono consentite) consulta cliccando qui le nostre F.A.Q.

MARIO DI MAURO

SICUREZZA NELLE COMUNICAZIONI SU RETE

Dai princìpi fondamentali ai paradigmi di nuova generazione, con esempi ed applicazioni pratiche

FrancoAngeli/Informatica

Per accedere all'allegato online è indispensabile
seguire le procedure indicate nell'area Biblioteca Multimediale
del sito www.francoangeli.it
registrarsi e inserire il codice **EAN 9788891760043** e l'indirizzo email
utilizzato in fase di registrazione

In copertina: *Sicurezza della rete globale. Vettore*,
© Maksim Pasko | Dreamstime.com

Indice

Introduzione

Da qualche anno a questa parte il concetto di "rete" è stato completamente rivoluzionato. Le informazioni, per acquisire un valore ancora più significativo, devono essere elaborate, processate, ricodificate ed aggregate. Queste informazioni sono già oggi sempre più eterogenee e provenienti da mondi differenti quali persone, oggetti intelligenti, mezzi di trasporto, processi e dati che formano un ecosistema che alcuni esperti definiscono Internet of Everything (IoE), ovvero, Internet del tutto. All'interno di questo contesto, i processi ed i meccanismi che governano la sicurezza delle informazioni diventano assolutamente indispensabili per due ragioni: la prima, ovvia, risiede nel fatto che al crescere del numero di interconnessioni di rete si moltiplica di conseguenza la quantità di minacce digitali. La seconda, invece, è legata all'eterogeneità di questo mastodontico ecosistema digitale che espone le risorse di rete più "deboli" ad una serie di rischi. Un sensore che trasmette informazioni utilizzando la rete internet, ad esempio, non potrà disporre di sofisticati meccanismi di sicurezza a causa delle risorse di calcolo fortemente limitate. Un software malevolo come un *malware* potrebbe quindi sfruttare questa vulnerabilità per attaccare il sensore, ed ottenere via libera per propagarsi all'interno della rete ad altri dispositivi.

Partendo dalla considerazione che i meccanismi in grado di trasportare sia informazioni utili che dannose su una rete dati sono gli stessi, questo libro offre una prospettiva della sicurezza dal punto di vista dello stack protocollare TCP/IP che, come è noto, rappresenta lo standard universale per lo scambio delle informazioni digitali.

Il testo è stato organizzato come segue.

Il *capitolo 1* presenta una panoramica dei classici meccanismi di crittografia utilizzati sulle reti dati, fino a tecniche più moderne come la crittografia omomorfa impiegata nell'ambito del cloud computing.

Nel *capitolo 2* si analizzano le vulnerabilità dei vari livelli dello stack protocollare TCP/IP, e vengono dettagliati alcuni attacchi di rete specifici per ogni livello della pila protocollare.

Il *capitolo 3* è dedicato ai sistemi di protezione da attacchi di rete, dove si ripercorre la suite TCP/IP individuando i criteri, i meccanismi ed i dispositivi più adatti ad intervenire sui vari livelli protocollari, anche con esempi pratici di configurazione.

Il *capitolo 4* presenta le caratteristiche di un software opensource indispensabile quando si parla di sicurezza su reti: Wireshark. Il capitolo è ricco di esempi e di configurazioni pratiche da testare immediatamente su rete.

Il *capitolo 5* introduce il concetto di statistiche di rete, ovvero, informazioni aggregate dalle quali ricavare comportamenti non immediatamente deducibili da analisi di traffico classiche. Anche in questo caso ci si avvale di Wireshark.

Il *capitolo 6* propone un dettagliato excursus sulle reti mobili fino ad arrivare al paradigma 5G ed analizzarne le caratteristiche sia sotto il profilo strutturale che sotto il profilo della sicurezza.

Il *capitolo 7*, infine, è dedicato al mondo dell'Internet of Things (IoT) di cui si analizzano nel dettaglio le caratteristiche di sicurezza dei principali protocolli.

Il testo è rivolto a coloro che conoscono i princìpi di base delle reti dati (professionisti, studenti di informatica o ingegneria, tecnici delle reti) e, oltre ad offrire suggerimenti pratici sulla messa in campo di soluzioni di sicurezza, propone approfondimenti sui protocolli di rete di moderna concezione che si stanno imponendo nel panorama attuale degli standard ICT e che costituiscono oramai il punto di partenza per affrontare le sfide tecnologiche del futuro.

1. Princìpi di sicurezza nelle comunicazioni su rete

1. Introduzione

Quando parliamo di comunicazione in senso lato, ci riferiamo tipicamente ad uno scenario nel quale intervengono tre attori principali: un mittente che rappresenta l'origine dell'informazione da trasmettere, un destinatario che sarà in grado di ricevere (e comprendere) l'informazione inviata dal mittente, ed infine un canale di comunicazione che rappresenta il mezzo attraverso il quale l'informazione viene trasmessa. Quando si introduce il tema della sicurezza nelle comunicazioni, bisogna necessariamente aggiungere un altro attore: l'intruso, ovvero quell'entità che a vario titolo può intromettersi all'interno della catena di comunicazione allo scopo di manipolare l'informazione.

In questo capitolo affronteremo i meccanismi di sicurezza e le contromisure che consentono di neutralizzare (o quanto meno di mitigare) le intenzioni dell'intruso e far sì quindi che le informazioni scambiate tra il mittente ed il destinatario possano essere comprensibili soltanto ai diretti interessati senza il rischio di manipolazioni indesiderate.

Quando trasferiamo i concetti di sicurezza di una comunicazione (universalmente validi) nel mondo delle reti dati, ci troviamo di fronte ad una varietà di casi e tipologie che non sempre possono essere trattati alla stessa maniera. Una comunicazione su rete dati potrebbe coinvolgere due utenti che scambiano dati attraverso una e-mail usando due personal computer, oppure due utenti che utilizzano servizi di chiamate vocali su IP (il cosiddetto VoIP) tramite due smartphone, o ancora due sensori che scambiano informazioni su alcune grandezze fisiche (es. temperatura, pressione, percentuale di anidride carbonica

nell'aria) utilizzando una rete dati. In tutti e tre gli esempi citati si potrebbe richiedere che le informazioni trasferite siano adeguatamente protette applicando princìpi di sicurezza che dovranno essere necessariamente differenti. Un sensore ad esempio, a differenza di un personal computer, non dispone di capacità elaborative tali da implementare meccanismi di sicurezza sofisticati, ma probabilmente ci si potrà accontentare di un livello di sicurezza della comunicazione non elevatissimo per il tipo di dati che deve trattare.

Ecco quindi che le prime domande da porsi quando si decide di progettare ed implementare un sistema di sicurezza su rete sono: quanto è importante l'informazione da trasmettere? Le entità che intervengono nella comunicazione sono in grado di supportare il livello di sicurezza richiesto? Quali sono le conseguenze derivanti dall'intromissione di un potenziale intruso?

Cercheremo di rispondere a queste domande attraverso una panoramica generale dei meccanismi che governano la sicurezza delle informazioni, mentre si rimanda a testi specifici (Stallings, 2017; Migga Kizza, 2017) per ulteriori approfondimenti tecnici.

2. Obiettivi della sicurezza su reti

Una comunicazione si definisce sicura quando è in grado di garantire quattro obiettivi fondamentali: confidenzialità, integrità, autenticazione e non ripudio. Iniziamo ad analizzare nel dettaglio questi quattro obiettivi.

2.1. Confidenzialità

Una comunicazione viene definita *confidenziale* quando risulta intellegibile soltanto ai diretti interessati, ovvero al mittente ed al destinatario. Un eventuale intruso, che abbia modo di intercettare la comunicazione (o parte di essa), la troverebbe incomprensibile. L'obiettivo di confidenzialità si raggiunge attraverso l'implementazione di meccanismi di crittografia che garantiscono l'intellegibilità della comunicazione alle sole entità effettivamente coinvolte.

2.2. Integrità

Una comunicazione si definisce *integra* quando non ha subìto manipolazioni esterne. Potrebbe infatti succedere che le informazioni transitanti su un canale di comunicazione siano recuperate da un intruso, decodificate, ed in seguito reimmesse sul canale di comunicazione in modo che il destinatario della comunicazione riceva un'informazione alterata.

A differenza della perdita di confidenzialità che coinvolge un intruso che intercetta passivamente la comunicazione, in questo caso l'intruso agisce attivamente attraverso la manipolazione fraudolenta dell'informazione. L'integrità dell'informazione viene tipicamente garantita attraverso l'applicazione delle funzioni di *hash* (par. 3.2.4).

2.3. Autenticazione

Attraverso la procedura di *autenticazione*, un utente viene semplicemente identificato. Tale identificazione può avvenire attraverso l'uso (eventualmente combinato) di varie procedure come: username e password, localizzazione geografica, utilizzo di smart card, utilizzo di codici temporanei (OTP – One Time Password), utilizzo di sensori biometrici (riconoscimento della retina, dell'impronta digitale etc.). Un utente correttamente autenticato viene quindi riconosciuto come un'entità fidata all'interno di una comunicazione.

2.4. Non ripudio

Il *non ripudio* fa riferimento all'impossibilità che, all'interno di una comunicazione, un utente dichiari di non averne preso parte. Qualora lo dichiari, dovrà dimostrare che il suo sistema di sicurezza è stato compromesso, e che quindi un potenziale intruso abbia preso la sua identità. Il servizio di non ripudio viene tipicamente garantito attraverso la firma digitale (par. 4) ed ha altresì implicazioni nel campo dell'informatica giuridica.

3. Cenni di crittografia

Il termine "crittografia" deriva dall'unione di due parole di origine greca: *kryptòs* ovvero "nascosto", e *graphìa* che significa "scrittura". Con questo termine si fa riferimento all'insieme di tecniche, metodi e regole che consentono di trasformare un testo in chiaro (ovvero intellegibile a tutti coloro che ne vengano in possesso) in un testo cifrato (o crittografato) che può essere decifrato soltanto da chi possiede uno strumento di decodifica (generalmente una chiave).

Nelle moderne reti di telecomunicazioni è impensabile immaginare che le informazioni possano viaggiare in chiaro, con il concreto rischio che un potenziale intruso possa intromettersi all'interno della comunicazione e collezionare in maniera fraudolenta i messaggi destinati ad un'altra entità. Vale forse la pena ricordare che nelle reti a commutazione di pacchetto (ad es. internet), a differenza delle reti a commutazione di circuito, le informazioni viaggiano seguendo percorsi differenti e non sempre predicibili. Basti pensare alla differenza che intercorre tra una telefonata tradizionale, nella quale la voce digitalizzata attraversa un "circuito" più o meno prestabilito, ed una telefonata VoIP (es. Skype) dove la voce digitalizzata viene suddivisa in pacchetti che viaggiano seguendo percorsi diversi secondo logiche di instradamento fornite dai *router*; non tutti questi percorsi sono controllabili e non è quindi così difficile per un esperto di "hacking" intercettare parte di questa comunicazione. Se questa comunicazione viene protetta attraverso meccanismi di crittografia, l'intruso non riesce a decodificarne il contenuto, a meno che non abbia a disposizione una chiave di decodifica.

Nelle reti attuali, i meccanismi di crittografia che vengono utilizzati sono variegati e dipendono dal tipo di applicazione che si utilizza. Strumenti come l'e-mail, programmi di instant messaging (es. WhatsApp), applicazioni VoIP (es. Skype), terminali di telefonia mobile, browser e App per la gestione di servizi come l'home banking, utilizzano in maniera nativa degli algoritmi crittografici, senza che l'utente debba preoccuparsi della gestione delle chiavi di codifica e decodifica. In una chiamata cellulare su rete UMTS (cap. 6 par. 3.2), ad esempio, le chiavi crittografiche sono immagazzinate nella scheda telefonica (USIM) e nell'Authentication Center (AuC), ovvero, il nodo dell'ope-

ratore deputato alla gestione dei meccanismi di sicurezza. Tale configurazione consente ad un utente di effettuare una telefonata preservando la privacy, pur senza conoscere la chiave di codifica (per cifrare la conversazione trasmessa) né quella di decodifica (per decifrare la conversazione ricevuta). La modalità di creazione, distribuzione e gestione delle chiavi crittografiche (sia di codifica che di decodifica) consente di distinguere due tipi di crittografia: la crittografia **simmetrica** e la crittografia **asimmetrica**.

3.1. Crittografia simmetrica

La crittografia simmetrica (o crittografia a singola chiave) si basa sull'utilizzo di un'unica chiave per cifrare e decifrare le informazioni. Lo schema di un modello a crittografia simmetrica è riportato in Figura 1 dove gli elementi di base sono:

- *testo in chiaro:* rappresenta il messaggio originale da trasmettere e costituisce l'input dell'algoritmo di cifratura;
- *algoritmo di cifratura:* è l'algoritmo che, a seguito di operazioni come trasformazioni e sostituzioni, è in grado di trasformare un testo in chiaro in un testo cifrato;
- *chiave segreta:* è un parametro fornito in ingresso all'algoritmo (e indipendente sia dal particolare algoritmo che dal testo in chiaro) che regola i meccanismi di trasformazione e sostituzione operati dall'algoritmo;
- *testo cifrato:* rappresenta il messaggio crittografato (in genere si presenta come una stringa di caratteri senza significato) che dipende dal testo in chiaro e dalla chiave segreta;
- *algoritmo di decifratura:* è l'algoritmo (inverso dell'algoritmo di cifratura) che permette ad un destinatario di poter recuperare il messaggio originale a partire da quello cifrato, grazie all'utilizzo della chiave segreta.

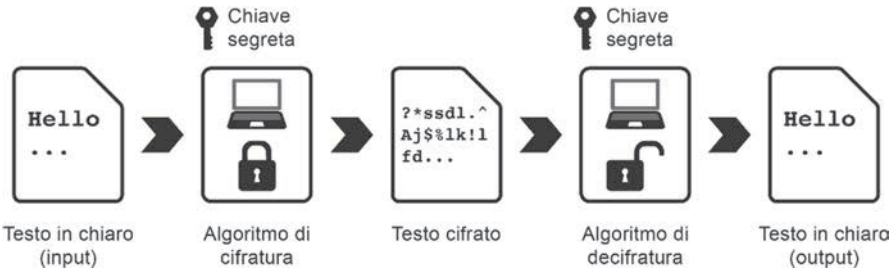

Figura 1 – Schema di crittografia simmetrica. Le chiavi per cifrare e decifrare l'informazione sono le stesse.

3.1.1. Un classico algoritmo a chiave simmetrica: il DES

L'algoritmo Data Encryption Standard (DES) trasforma i dati in chiaro a partire da blocchi di bit, utilizzando una combinazione di sostituzioni (trasformazioni di bit in altri bit) e permutazioni (trasposizioni di bit in posizioni differenti) per crittografare i dati. La chiave di cifratura (che coincide con quella di decifratura) viene combinata tramite funzioni XOR con i dati in chiaro che rappresentano l'input dell'algoritmo DES.

La Figura 2 riporta uno schema semplificato dell'algoritmo. L'informazione da cifrare (testo in chiaro) viene suddivisa in blocchi da 64 bit che subiscono una permutazione iniziale. La chiave utilizzata per la cifratura è da 64 bit, sebbene ne vengano utilizzati soltanto 56 dal momento che i restanti 8 bit sono di "parità", ovvero, rappresentano un codice di controllo utilizzato per prevenire errori nella memorizzazione (o nella trasmissione) della chiave stessa. A partire dalla chiave iniziale, vengono generate 16 sotto-chiavi attraverso operazioni di spostamento di bit (shift circolari) ed operazioni di permutazione. A questo punto, un blocco di funzioni (dette di *round*) combinano, attraverso delle operazioni XOR, le 16 sotto-chiavi generate con l'informazione in uscita dal blocco di permutazione iniziale ed ulteriormente elaborata. L'output del blocco che opera attraverso le funzioni di *round* viene dato in ingresso ad un ulteriore blocco che esegue l'operazione inversa a quella della permutazione iniziale, producendo così un messaggio cifrato di 64 bit.

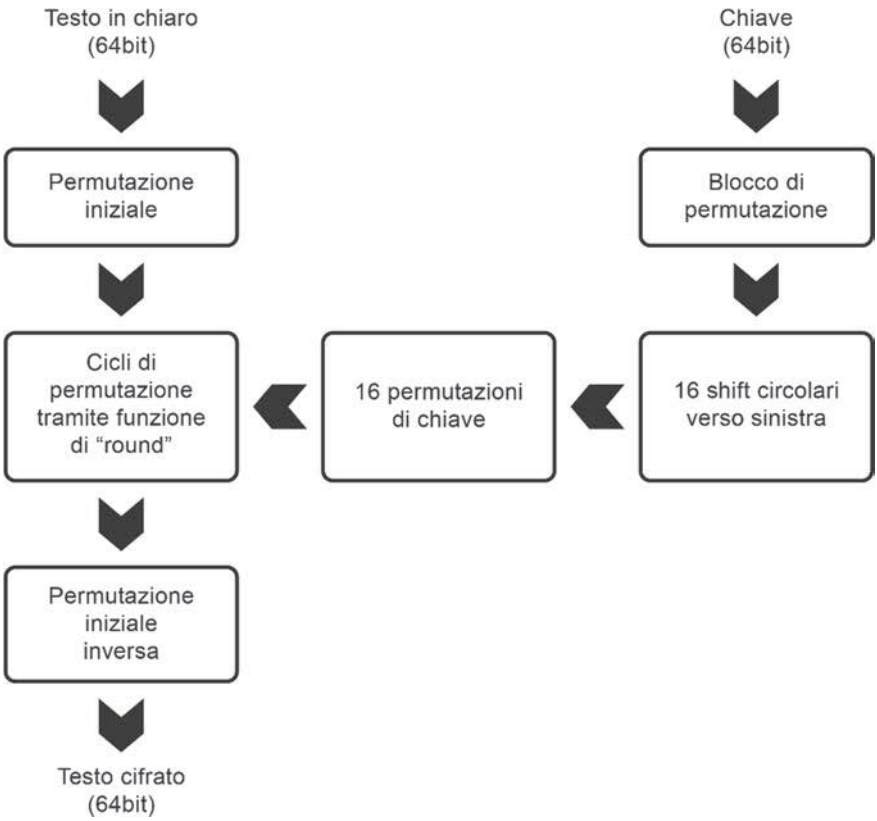

Figura 2 – Schema di funzionamento dell'algoritmo DES. A partire da un testo in chiaro (suddiviso in blocchi da 64 bit), si applica una chiave da 56 bit (8 bit sono usati per la parità) e si ottiene un testo cifrato (blocco da 64 bit).

Attualmente, il DES viene considerato un algoritmo poco sicuro soprattutto per la lunghezza della chiave che lo rende scarsamente robusto. Un attacco di tipo *brute force* (ovvero un attacco che esplora tutto lo spazio possibile delle chiavi) dovrebbe esplorare 2^{56} chiavi, che corrisponde all'incirca a $7{,}2056 \cdot 10^{16}$ chiavi. Supponendo di disporre di un processore da 1 MHz che possa testare una chiave ad ogni ciclo di clock (ovvero di un processore che sia in grado di provare una chiave ogni 10^{-6} secondi), il tempo per provare tutte le possibili chiavi ammonterebbe a poco più di 1142 anni (2^{55} μsec). Un processore da 1 GHz (una chiave ogni 10^{-9} secondi), invece, impiegherebbe poco più di un anno, mentre un processore con una velocità di 1 THz (che cor-