Sicurezza nelle reti

A.A. 2005/2006

Walter Cerroni

Sicurezza delle informazioni: definizione

- Garantire la **sicurezza** di un sistema informativo significa impedire a potenziali soggetti attaccanti **l'accesso o l'uso non autorizzato** di informazioni e risorse

- Un attacco ad un sistema informativo può portare a
  - parziale o totale distruzione di informazioni
  - parziale o totale rivelazione di informazioni riservate
  - furto o utilizzo indebito di uno o più servizi
  - negazione di uno o più servizi agli utenti del sistema
- I fini di questo tipo di attacco possono essere
  - pura sfida
  - guadagno politico o economico
  - volontà di danneggiare una istituzione

2

Sicurezza delle informazioni: problematiche

- **Autenticazione** (authentication)
  - verificare l'identità di un utente tramite:
    - possesso di un oggetto (chiave o smart card)
    - conoscenza di un segreto (password)
    - caratteristica personale fisiologica (impronta digitale)
  - verificare l'autenticità di un messaggio
- **Autorizzazione** (authorisation)
  - specificare le azioni consentite a ciascun utente
- **Riservatezza** (privacy)
  - impedire l'accesso alle informazioni da parte di utenti non autorizzati

3

Sicurezza delle informazioni: problematiche

- **Integrità** (integrity)
  - impedire la modifica non autorizzata (accidentale o deliberata) delle informazioni
- **Disponibilità** (availability)
  - garantire in qualunque momento la possibilità di usare le risorse a chi ne è autorizzato
- **Paternità** (non-repudiability)
  - impedire ad un utente di ripudiare un suo messaggio

4

Sicurezza nei sistemi informativi distribuiti

- Un moderno sistema informativo è composto da informazioni che risiedono su host collegati in rete ed eventualmente da più reti interconnesse
- Sicurezza: proteggere sia informazioni che risorse di rete
- Si deve quindi distinguere fra:
  - **sicurezza sugli host**
  - **sicurezza nella rete**
- Le problematiche sono sostanzialmente le stesse
- La sicurezza sugli host e in rete sono correlate:
  - un attacco riuscito su di un host può facilitare l'accesso alle informazioni in rete
  - un attacco riuscito alla rete può mettere in pericolo gli host connessi ad essa

5

Tipi di attacchi in rete

- **Intercettazione**
  - passiva: vengono letti i dati inviati in rete
  - attiva: vengono letti e modificati i dati inviati in rete
- **Intrusione**
  - accesso non autorizzato ad uno o più host
- **Furto di informazione**
  - appropriazione indebita di dati residenti su un host
- **Rifiuto di servizio**
  - vengono compromessi o disabilitati in modo non autorizzato alcuni servizi di rete

6

Strategie di protezione

- Sicurezza mediante oscurità
  - il sistema va configurato in modo tale da non essere visibile dall'esterno
- Sicurezza sulla rete
  - si vuole proteggere la rete nella sua globalità da attacchi esterni
- Sicurezza sull'host
  - ciascun host viene protetto separatamente, attraverso il sistema operativo o altro software locale
- Sicurezza a livello di applicazione
  - si garantisce la protezione dei dati tramite meccanismi integrati nelle applicazioni
- Nessun meccanismo di sicurezza
  - informazioni e risorse non sono considerate critiche dal punto di vista della sicurezza (ne siamo proprio sicuri?)

7

Sniffing e spoofing

- Esistono semplici software (**sniffer**) usati per intercettare i dati in transito sulla rete (decodificando i protocolli)
  - è possibile entrare in possesso di informazioni riservate trasmesse in chiaro (come le password) compromettendo la sicurezza degli host e la validità delle procedure di autenticazione
  - sono necessarie tecniche di **crittografia** dei dati sensibili
- Alcuni meccanismi di autenticazione si basano sull'indirizzo IP o MAC sorgente
  - è possibile forgiare datagrammi IP o trame MAC contenti un falso indirizzo sorgente (**spoofing**)
  - chi attacca riesce ad autenticarsi e ad eseguire applicazioni di rete e/o causare invio di dati non autorizzati
  - le risposte non tornano indietro, ma tramite sniffer si possono intercettare e leggere i dati trasmessi (se interessano)
  - sono necessarie tecniche avanzate di **autenticazione**

8

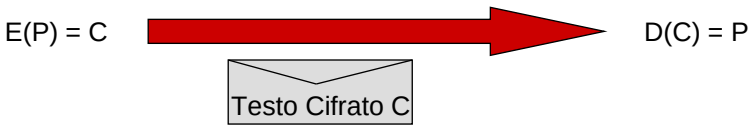
Uso di crittografia e autenticazione

- Tecniche fondamentali nelle strategie di protezione a livello di host e di applicazione
- La crittografia garantisce
  - riservatezza delle informazioni
  - integrità dei dati trasmessi
- L'autenticazione garantisce
  - identità dell'interlocutore remoto
  - autenticità delle informazioni
  - paternità delle informazioni

9

Crittografia

- L'idea di base è quella di trasformare un messaggio in modo tale che solo utenti autorizzati riescano a leggerlo



  - P: testo in chiaro (plain text), comprensibile a tutti
  - C: testo cifrato (ciphertext), comprensibile solo al destinatario
  - E: funzione di cifratura, capace di rendere il messaggio decifrabile solo dal destinatario
  - D: funzione di decifrazione utilizzata dal destinatario per leggere il messaggio cifrato (solo il destinatario la conosce)

10

Algoritmi di cifratura

- L'algoritmo di cifratura è la funzione matematica usata per cifrare e decifrare il messaggio
- **Algoritmi basati su carattere**
  - sostituzione
    - ogni simbolo si trasforma in un altro simbolo dell'alfabeto
    - cambiano i simboli ma non il loro ordine nel testo
  - trasposizione
    - i simboli vengono permutati in base ad una permutazione stabilita
    - i simboli dell'alfabeto non cambiano ma cambia l'ordine in cui compaiono nel messaggio
- **Algoritmi basati su chiave**
  - oltre a definire l'algoritmo, si usa una chiave per cifrare/decifrare
  - lo stesso algoritmo, con chiavi diverse, produce testi cifrati diversi a partire dallo stesso testo in chiaro

11

Sicurezza degli algoritmi a chiave

- Dato un sistema di crittografia a chiave, la sua sicurezza si fonda su
  - segretezza della chiave
  - segretezza dell'algoritmo
  - sicurezza dell'algoritmo se questo non è segreto
- In generale l'algoritmo di cifratura è noto
  - altrimenti bisognerebbe inventarne sempre di nuovi
  - nessun algoritmo è assolutamente sicuro (sistemi teoricamente sicuri sono irrealizzabili in pratica)
  - si deve rendere praticamente irrealizzabile l'attacco alle informazioni cifrate

12

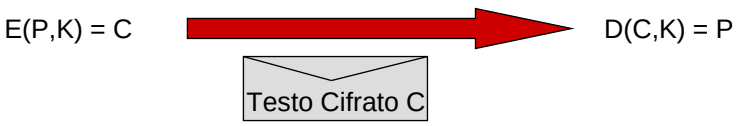
Attacco di forza bruta

- Quando l'algoritmo di cifratura è noto, si è esposti al cosiddetto **attacco di forza bruta**
  - si conosce l'algoritmo crittografico ma non la chiave
  - si applicano al messaggio cifrato tutte le possibili chiavi ottenendo tutti i possibili messaggi originali, fra cui anche quello vero
  - interpretando il significato si isola il vero messaggio originale all'interno dell'insieme di tutti i messaggi ottenuti
- L'attacco di forza bruta richiede uno sforzo di elaborazione molto elevato
  - garantisce il successo dell'attacco ma non i tempi necessari per ottenerlo
  - un algoritmo di cifratura si può considerare sicuro se il tempo necessario per completare un attacco di forza bruta è superiore al tempo di vita dell'informazione contenuta nel messaggio

13

Crittografia a chiave segreta (simmetrica)

- La chiave K è la stessa per cifrare e decifrare il testo e deve essere nota contemporaneamente a chi invia e a chi riceve il messaggio



- Le funzioni di cifratura e decifrazione sono una l'inversa dell'altra:

$$D(E(P,K) , K) = P$$
$$E(D(C,K) , K) = C$$

14

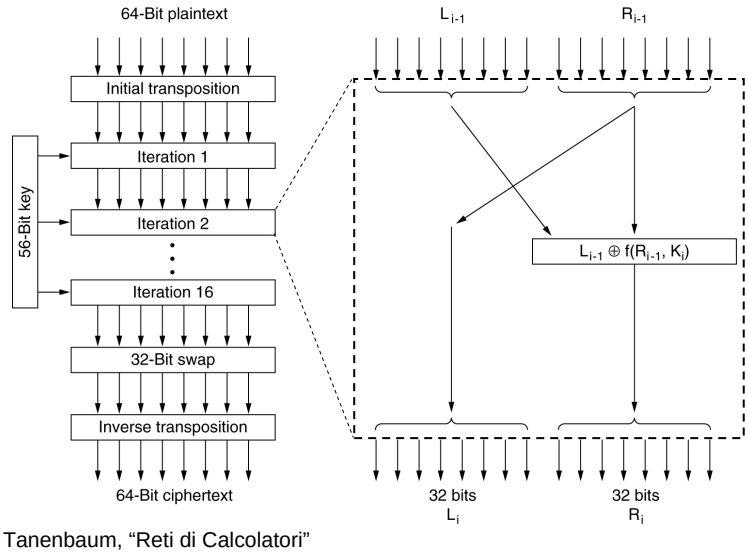
Algoritmi simmetrici e gestione della chiave

- Alcuni algoritmi a chiave segreta
  - DES (1977): chiave a 56 bit, ormai insicuro
  - Triple DES (1979): chiave a 168 bit
  - AES (1997): chiave a 128, 192 o 256 bit

- Lo scambio di informazioni cifrate può avvenire solo fra utenti a conoscenza della chiave
- Scelta la chiave un utente deve inviarla a chiunque debba comunicare con lui in modo sicuro
- Questa procedura è un potenziale punto debole del sistema di sicurezza

15

L'algoritmo di cifratura DES



Da A.S. Tanenbaum, "Reti di Calcolatori"

16

Crittografia a chiave pubblica (asimmetrica)

- Si usano due chiavi K_1 e K_2, una usata per cifrare l'altra per decifrare:

- La chiave di cifratura K_1 è resa nota (**chiave pubblica**)
- La chiave di decifrazione K_2 è segreta (**chiave privata**)
- E' praticamente impossibile dedurre K_2 da K_1
- Naturalmente deve valere $D(E(P,K_1), K_2) = P$

17

Crittografia a chiave pubblica: utilizzo

- I sistemi a chiave pubblica possono essere utilizzati per
  - assicurare la riservatezza del dialogo
    - Bob conosce la chiave pubblica di cifratura per Alice K_{1A}
    - Bob cifra il messaggio ed invia $E(P,K_{1A}) = C$
    - Alice riceve C e lo decifra con la chiave privata di decifrazione K_{2A} nota solo a lei: $D(C,K_{2A}) = P$
    - un ascoltatore non autorizzato non può decifrare i dati in quanto non conosce K_{2A}
  - autenticare il contenuto di un messaggio e garantirne la paternità
    - si suppone che $E(D(P,K_2), K_1) = P$
    - Bob cifra il messaggio con la sua chiave privata e poi lo invia ad Alice: $D(P,K_{2B}) = C$
    - Alice riceve C e lo decifra con la chiave pubblica di Bob, ottenendo $E(D(P,K_{2B}), K_{1B}) = P$
    - solo Bob può aver generato il messaggio $D(P,K_{2B})$

18

Algoritmo a chiave pubblica: RSA

- L'algoritmo più noto è conosciuto con l'acronimo RSA
  - da Rivest, Shamir, Adleman (1978)
- Le funzioni per cifrare e decifrare sono le stesse, cambia solamente la chiave
- Si utilizzano proprietà matematiche legate ai numeri primi
  - la chiave privata e la chiave pubblica sono funzione di numeri primi grandi (rappresentati con 1024 bit)
  - se si moltiplicano tra loro due numeri primi grandi, la fattorizzazione del prodotto di tali numeri è un problema computazionalmente molto complesso
  - la difficoltà nella definizione delle chiavi è la ricerca dei due numeri primi grandi, che richiede un notevole sforzo computazionale (ma va eseguito una tantum)

19

Crittografia a chiave pubblica: caratteristiche

- Per poter avviare una comunicazione sicura fra utenti non è necessaria alcuna transazione privata
- La chiave pubblica può essere pubblicata in un apposito elenco oppure semplicemente inviata all'inizio della comunicazione
- Tale tecnica ha un costo computazionale molto superiore a quello degli algoritmi simmetrici
  - si può usare per negoziare in modo sicuro una chiave simmetrica
- Non è sufficiente a salvaguardare uno degli interlocutori da un eventuale comportamento malevolo dell'altro
  - esempio: si invia una transazione bancaria per un valore di 10; il ricevente, dopo aver decifrato il messaggio, modifica 10 in 100: non c'è modo di dimostrare chi ha ragione

  → si introduce il concetto di **firma elettronica**

20

Firma elettronica

- Come per la firma tradizionale, si deve garantire che
  - la firma sia autentica
  - la firma non sia falsificabile
  - il documento firmato non sia alterabile
  - la firma non sia riusabile in un altro documento
  - la firma non possa essere disconosciuta
- Deve essere quindi
  - dipendente dall'identità del firmatario
    - l'uso di un meccanismo a chiave pubblica permette l'autenticazione e garantisce la paternità
  - dipendente dal messaggio
    - si cifra un sunto del messaggio ottenuto tramite una **funzione hash**
    - se si modifica il messaggio il sunto risulta diverso
    - algoritmi usati: MD5, SHA

21

Firma elettronica

- Alice vuole inviare un messaggio firmato a Bob
  - usa una funzione hash nota per generare un sunto del messaggio
  - cifra il sunto con la sua chiave privata generando la **firma**
  - invia il messaggio (cifrato o meno) unitamente alla firma
- Bob riceve il messaggio e ne ricalcola il sunto
  - solo con la chiave pubblica di Alice è in grado di decifrare la firma
  - può verificare l'autenticità, la paternità e l'integrità del messaggio confrontando il sunto ottenuto con il risultato della decifrazione della firma
- Per il destinatario non è possibile
  - modificare il messaggio alla ricezione sostenendone l'autenticità
- Per il mittente non è possibile
  - ripudiare la paternità di un messaggio
  - modificare il messaggio dopo averlo inviato e sostenerne l'autenticità

22

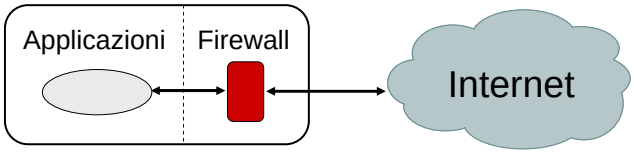
Autenticità delle chiavi

- L'elenco delle chiavi pubbliche è un potenziale punto debole per la sicurezza del sistema
- Esiste il problema della autenticità delle chiavi pubbliche
  - un utente può in malafede pubblicare una chiave a nome di un altro ed utilizzarla per sostituirsi a lui
- Si ricorre a terze parti, dette **Certification Authority**, che garantiscono l'integrità e l'autenticità dell'elenco delle chiavi pubbliche (racc. ITU X.509)
  - la Certification Authority deve essere al di sopra di ogni sospetto, compatibilmente con il livello di sicurezza desiderato
  - la Certification Authority genera un **certificato** contenente la chiave pubblica dell'utente e lo firma con la propria chiave privata
  - qualunque altro utente può verificare che il certificato sia stato effettivamente firmato dall'Authority

23

Protezione di host: personal firewall

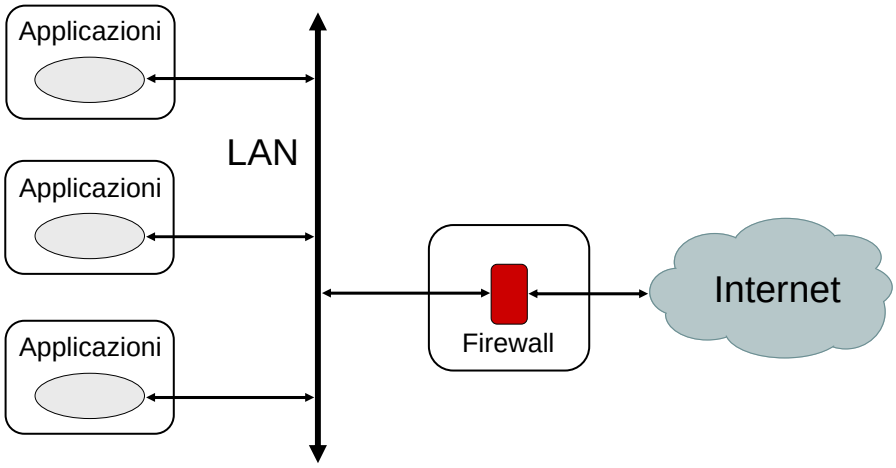
- Un firewall è un filtro software che serve a proteggersi da accessi indesiderati provenienti dall'esterno della rete
- Può essere semplicemente un programma installato sul proprio PC che protegge quest'ultimo da attacchi esterni



24

Protezione di rete: firewall

- Oppure può essere una macchina dedicata che filtra tutto il traffico da e per una rete locale



25

Protezione di rete: firewall

- Tutto il traffico fra la rete locale ed Internet deve essere filtrato dal firewall
- Solo il traffico autorizzato deve attraversare il firewall
- Si deve comunque permettere che i servizi di rete ritenuti necessari siano mantenuti
- Il firewall deve essere per quanto possibile immune da problemi di sicurezza sull'host
- In fase di configurazione di un firewall, per prima cosa si deve decidere la politica di default per i servizi di rete
  - **default deny**: tutti servizi non esplicitamente permessi sono negati
  - **default allow**: tutti i servizi non esplicitamente negati sono permessi

26

Livelli di implementazione

- Un firewall può essere implementato come
  - packet filter
  - proxy server
    - application gateway
    - circuit-level gateway
- **Packet filter**
  - si interpone un router fra la rete locale ed Internet
  - sul router si configura un filtro sui datagrammi IP da trasferire attraverso le varie interfacce
  - il filtro scarta i datagrammi sulla base di
    - tipo di servizio a cui il datagramma è destinato (porta TCP/UDP oppure campo PROTOCOL)
    - indirizzo IP sorgente o destinazione
    - indirizzo MAC sorgente o destinazione
    - interfaccia di provenienza o destinazione

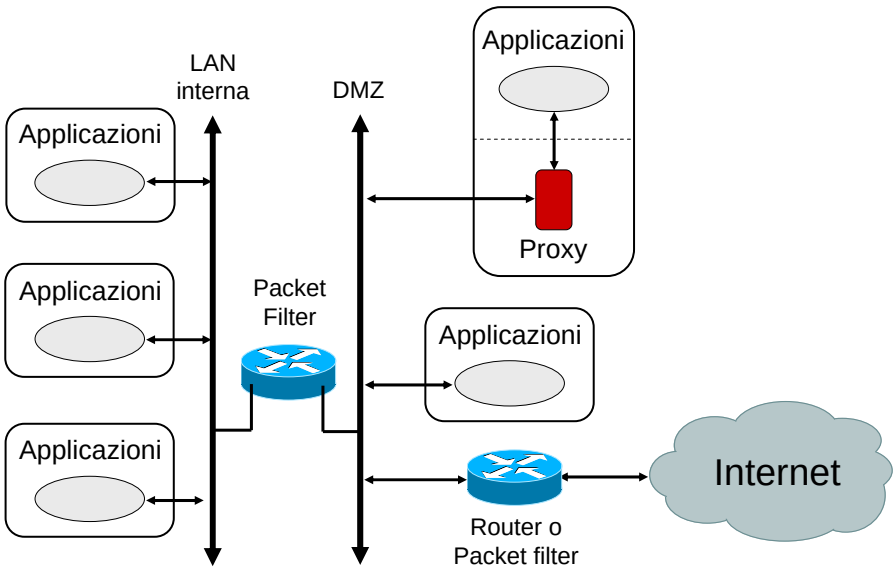
27

Livelli di implementazione

- **Proxy server**
  - esempio: nella rete protetta l'accesso ad Internet è consentito solo ad alcuni host
  - si interpone un server apposito detto proxy server per realizzare la comunicazione per tutti gli host
  - il proxy server evita un flusso diretto di datagrammi fra Internet e le macchine della rete locale
  - **application level**
    - viene impiegato un proxy server dedicato per ogni servizio che si vuole garantire
  - **circuit level gateway**
    - è un proxy server generico in grado di inoltrare le richieste relative a molti servizi

28

Configurazione di packet filter e proxy



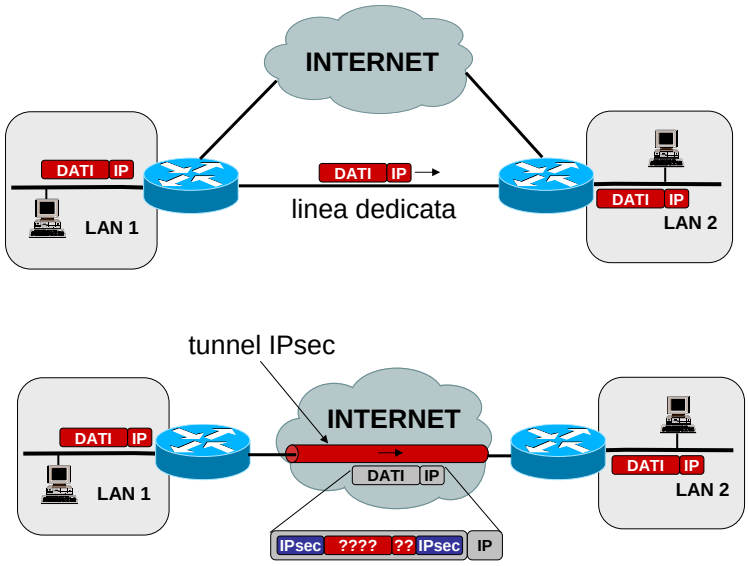
29

Reti private e reti private virtuali

- Aziende e/o enti di dimensioni medio/grandi in genere hanno necessità di interconnettere in maniera sicura sedi sparse sul territorio e distanti tra loro
- Soluzione tradizionale: utilizzo di linee dedicate da affittare direttamente presso gli operatori (**reti private**)
  - soluzione in genere costosa
- Alternativa più economica: utilizzo di tunnel sicuri attraverso reti pubbliche (**reti private virtuali** - **VPN**)
  - flusso punto-punto di pacchetti autenticati (con contenuto informativo cifrato) incapsulati in pacchetti tradizionali
  - diverse tecnologie disponibili
  - protocolli di tunnelling
    - livello 2: PPTP, L2TP
    - livello 3: IPsec

30

Reti private IP e reti private virtuali IPsec



31