Cenni sulla sicurezza nelle reti

Gennaro (Rino) Vessio
gennaro.vessio@uniba.it

Etimologia

- Il termine «sicurezza» deriva dal latino
  - «sine cure»: senza preoccupazioni
- NON siamo interessati alla sicurezza dal punto di vista del cugino che sfascia il PC, ma dal punto di vista logico
  - il sistema deve comportarsi come auspicato

2

Accezione

- Tuttavia in italiano collassano due accezioni che in altre lingue, p.e. l'inglese, sono denotate da termini differenti:
  - safety: qualcosa di «indesiderato» non deve mai accadere
  - security: il sistema deve essere «protetto» da minacce
- Noi siamo interessati alla seconda

3

Principio generale

«*Una catena è forte quanto il suo anello più debole*»

- Progettare un sistema sicuro NON è banale: una minima incrinatura può compromettere la sicurezza dell'intero sistema
  - una rete di calcolatori è un sistema critico e complesso

4

Due punti di vista

- Possiamo considerare il problema della sicurezza sotto due punti di vista:
  - la sicurezza dei propri dati
  - la sicurezza delle proprie comunicazioni

5

LA SICUREZZA DEI PROPRI DATI

6

Password

- Tipicamente associata a uno username, una password è una stringa alfanumerica per accedere a servizi che richiedono una identificazione univoca
- All'account di un utente sono anche associate autorizzazioni:
  - l'utente gode di determinati permessi e privilegi

7

Problemi

- Stessa password per servizi diversi
- Password vulnerabili (dati anagrafici, parole di senso compiuto, etc.)
- Password inalterate
- Password annotate (su file, su pezzi di carta, etc.)

8

Alcune fra le password più utilizzate

- 123456
- password
- qwerty
- iloveyou
- 000000
- 111111
- starwars

9

Virus

- Un virus è un programma concepito per arrecar danno
- Esattamente come un virus biologico, il suo scopo è auto-replicarsi per diffondersi il più possibile nell'organismo ospite
- Uno dei mezzi privilegiati per la diffusione di virus è la posta elettronica

10

«Sintomi» frequenti

- Rallentamento delle prestazioni
- Impossibilità di accedere a file
- Scomparsa di file o cartelle
- Impossibilità di eseguire un programma
- Non funzionamento di componenti hardware
- …

11

Alcuni tipi di virus

- Malware: virus auto-replicante che usa la rete per propagarsi
- Trojan: particolare virus che si nasconde dietro un'applicazione che sembra essere lecita
  - qual è la metafora qui?
- Spyware: virus concepito per raccogliere informazioni dalla macchina ospite
- Backdoor: virus che permette un accesso non autorizzato da remoto

12

Sfatiamo un mito

- Non è possibile programmare un virus da iniettare nel sistema informatico centrale di un'astronave madre aliena…

13

Meccanismi di protezione (1)

- Gli anti-virus tradizionali monitorano i file su disco confrontandoli con virus catalogati in archivi
  - è possibile riconoscere solo virus già noti
- Anti-virus sperimentali usano metodi statistici per individuare potenziali virus
  - maggiore tasso di falsi positivi

14

Meccanismi di protezione (2)

- I firewall filtrano i pacchetti entranti da e uscenti verso una rete
  - implementano politiche di controllo e monitoraggio, confrontando i dati in transito con profili predefiniti
- Ne esistono sia hardware che software

15

LA SICUREZZA DELLE PROPRIE COMUNICAZIONI

16

Comunicazione

- Una comunicazione coinvolge (almeno) due soggetti:
  - mittente
  - destinatario
- Consiste nello scambio di messaggi (o pacchetti)
- Avviene su di un mezzo trasmissivo (canale)
- Un canale è intrinsecamente non sicuro

17

Proprietà e minacce

- La sicurezza delle proprie comunicazioni può essere considerata sotto due punti di vista:
  - il soddisfacimento di determinate proprietà
  - la protezione da determinate minacce

18

Proprietà

- Confidenzialità: nessun intruso può leggere i messaggi scambiati
- Autenticazione: delle entità coinvolte nella comunicazione
- Integrità: garanzia che i messaggi non siano stati corrotti
- Non ripudio: non deve essere possibile negare di aver partecipato a una comunicazione
- Anonimia (non sempre): deve poter non essere rivelata la propria identità

19

Minacce

- Intercettazioni: un intruso ottiene accesso a dati segreti
- Interruzioni: i servizi o i dati diventano inutilizzabili (p.e. attacco DoS)
- Alterazioni: cambiamenti non autorizzati ai dati
- Contraffazioni: vengono generati dati aggiuntivi che normalmente non esisterebbero

20

Meccanismi di protezione

- Per soddisfare tali proprietà o per proteggersi da tali minacce, si adottano due meccanismi fondamentali:
  - crittografia
  - protocolli di autenticazione

21

Crittografia

- Etimologicamente, il termine «crittografia» deriva dal greco
  - «kryptós graphía»: scrittura nascosta
- L'idea è intuitiva: si codifica un messaggio in chiaro, intelligibile da chiunque, in un messaggio cifrato, intelligibile solo dal destinatario

22

Il cifrario di Cesare

- La crittografia era nota già agli antichi, tant'è che uno dei primi cifrari risale all'Antica Roma
- Cifrario di Cesare: si sostituisce ciascuna lettera con quella che segue di tre posizioni nell'alfabeto

«*attaccare gli irriducibili galli alla ora sesta*»

↓

«*dzzdffduh lon nuungafnenon ldoon dood rud vhzd*»

23

La chiave

- Abbiamo quindi due componenti:
  - un algoritmo di cifratura
  - un algoritmo di decifratura
- Nel cifrario di Cesare il parametro comune ai due algoritmi, la chiave di cifratura e decifratura, è il numero 3
- Principio di Kerckhoofs:

«*La chiave è l'unica vera informazione che occorre tenere segreta*»

24

Assunzione di cifratura perfetta

- L'equivalente di tale principio è l'assunzione di cifratura perfetta:
  «*Si può riottenere il contenuto in chiaro solo conoscendo l'opportuna chiave di decifratura*»
  – gli algoritmi sono spesso resi noti, soprattutto per studiarne le debolezze
- L'assunzione si fonda sull'inviolabilità della chiave impiegata
- Infine, quest'ultima si fonda sull'intrattabilità computazionale del metodo forza bruta

25

Metodo forza bruta

- Si provano sistematicamente ed esaustivamente tutte le possibili chiavi fino a trovare quella corretta
- Immaginiamo di avere una valigetta sbloccabile da un numero a tre cifre decimali:
  – nel peggiore dei casi qual è il numero di tentativi?

26

Complessità del metodo

- La complessità computazionale in tempo del metodo forza bruta è asintoticamente $O(2^n)$ dove n è la lunghezza in bit della chiave
  – il problema è NP-completo

Power / cost	40 bits (5 char)	56 bits (7 char)	64 bits (8 char)	128 bits (16 chars)
$ 2K (1 PC. Can be achieved by an individual)	1.4 min	73 days	50 years	10^{20} years
$ 100 K (This can be achieved by a company)	2 sec	35 hours	1 year	10^{19} years
$ 1 M (Achieved by a huge organization or a state)	0.2 sec	3.5 hours	37 days	10^{18} years

Fig 4 Estimate time for successful brute-force attack

27

Sfatiamo un mito

- Non è possibile forzare una chiave con la semplice pressione compulsiva dei tasti
- Teorema della scimmia instancabile: benché la probabilità di riprodurre un testo prefissato componendo caratteri a caso è 1, occorre un tempo che tende a infinito

28

Crittografia simmetrica

- Anche detta a chiave privata, in essa le chiavi di cifratura e decifratura coincidono (o, al più, sono direttamente ricavabili l'una dall'altra)
  - il cifrario di Cesare ne è un esempio
- Formalmente, $\forall M, \forall K: D{\downarrow}K\,(E{\downarrow}K\,(M)) = M$

29

Limitazione

- La conoscenza della chiave dev'essere condivisa dalle parti comunicanti a priori
  - incontro per concordare la chiave (spesso infattibile)
  - trasmissione della chiave lungo il canale (di per sé inaffidabile)

30

Indovinello

- Una persona deve spedire un diamante ad un amico
- Lo ripone in una cassaforte inattaccabile
- La cassaforte può essere chiusa con un lucchetto
- Non c'è modo di aprire la cassaforte se non con la chiave del lucchetto
- Come inviare la chiave in modo sicuro?

31

Soluzione

- L'amico spedisce un proprio lucchetto aperto di cui già dispone della chiave
- Il proprietario del diamante invia la cassaforte chiusa dal lucchetto dell'amico
- Solo quest'ultimo potrà aprirla

32

Crittografia asimmetrica

- Anche detta a chiave pubblica, le chiavi di cifratura e decifratura sono diverse (pur costituendo una coppia inscindibile)
  - il destinatario rende pubblica la chiave con cui cifrare messaggi
  - è l'unico conoscitore della chiave di decifratura con cui decifrarli
- Meno efficiente dal punto di vista computazionale

33

Formalmente

- Il sistema deve godere delle seguenti proprietà:
  - $D{\downarrow}Ks\,(E{\downarrow}Kp\,(M))=M$
  - sia $E{\downarrow}Kp$ che $D{\downarrow}Ks$ sono facili da calcolare
  - pur conoscendo $E{\downarrow}Kp$, calcolare $D{\downarrow}Ks$ a partire da $E{\downarrow}Kp$ è infattibile
- La complessità del problema di calcolare $D{\downarrow}Ks$ dev'essere equivalente alla complessità del metodo forza bruta

34

Algoritmo RSA (1)

- Algoritmo di generazione delle chiavi:
  - si generano casualmente due numeri primi molto grandi, p e q
  - si calcola $n = pq$
    - la lunghezza in bit di n è la lunghezza in bit della chiave, p.e. 1024 bit nell'attuale standard di sicurezza
  - si calcola $\varphi(n) = (p - 1)\,(q - 1)$
    - $\varphi(n)$ è la funzione totiente di Eulero
  - si sceglie un intero e, $1 < e < \varphi(n)$, tale che $\text{mcd}(e, \varphi(n)) = 1$
    - si dice che e e $\varphi(n)$ sono coprimi
  - si sceglie d, $1 < d < \varphi(n)$, tale che $ed \equiv 1 \pmod{\varphi(n)}$

35

Algoritmo RSA (2)

- La coppia (n, e) è la chiave pubblica
- La coppia (n, d) è la chiave privata
- Algoritmo di cifratura:
  - dato $m \in M$, lo si rappresenta con un intero
  - si calcola $c = m^e \pmod{n}$
- Algoritmo di decifratura:
  - si calcola $m = c^d \pmod{n}$

36

Algoritmo RSA (3)

- $ed \equiv 1 \pmod{\varphi(n)} \rightarrow d \equiv e^{-1} \pmod{\varphi(n)}$
- Per calcolare d NON basta e ma serve conoscere $\varphi(n) = (p-1)(q-1)$:
  - $n = pq$, con p e q numeri primi molto grandi…
  - … ma la fattorizzazione in numeri primi di numeri molto grandi è un problema intrattabile!

37

Algoritmo RSA (4)

- La correttezza dell'algoritmo si dimostra applicando il piccolo teorema di Fermat e il teorema cinese del resto
  - si lascia come esercizio
- Per trasmettere grandi quantità di dati occorre molto tempo
  - soluzione: RSA viene usato SOLO per scambiare una chiave segreta usata poi come chiave di un sistema crittografico simmetrico

38

Esempio (1)

- $p = 3$, $q = 11$
- $n = pq = 3 \cdot 11 = 33$
- $\varphi(n) = (p-1)(q-1) = (3-1)(11-1) = 20$
- e ($< \varphi(n)$, coprimo con $\varphi(n)$) = 7
- d (inverso moltiplicativo di e mod $\varphi(n)$) = 3
  - infatti $ed \equiv 1 \pmod{\varphi(n)} \rightarrow 7 \cdot 3 = 21 \equiv 1 \pmod{20}$
- chiave pubblica: (33, 7)
- chiave privata: (33, 3)

39

Esempio (2)

- A = 1, B = 2, C = 3, …
- m = Q = 15
- $c = m^e \pmod{n} = 15^7 \pmod{33} = 27$
- $m = c^d \pmod{n} = 27^3 \pmod{33} = 15$

40

Crittografia post-quantistica

- RSA si fonda sull'intrattabilità del problema della fattorizzazione in numeri primi
  - ad oggi NON ne esiste una risoluzione efficiente utilizzando gli algoritmi classici
- Ma, se si disponesse di un computer quantistico sufficientemente potente, si potrebbe eseguire la fattorizzazione di Shor
  - la sua complessità è polinomiale
  - la sicurezza di RSA sarebbe compromessa
- Simulare un computer quantistico richiede un tempo esponenziale, per ora…

41

Problema

- Colui che rende pubblica la sua chiave di cifratura NON è sicuro dell'identità di chi comunica con lui
  - occorre un modo per autenticare le parti comunicanti

42

Protocolli di autenticazione

- L'obiettivo è l'instaurazione di un canale sicuro fra le parti comunicanti
- Un canale sicuro autentica mittenti e destinatari e li protegge da intercettazioni, alterazioni e contraffazioni

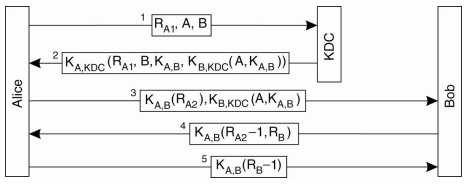
43

Key Distribution Center

- Si utilizza un approccio centralizzato appoggiandosi a un *key distribution center* (KDC) affidabile
  - esso assume il ruolo di terza parte fidata
  - condivide chiavi segrete con i processi
  - genera chiavi segrete di sessione su richiesta per permettere la comunicazione fra coppie di processi

44

Schema classico Needham-Schroeder



45

Nonce

- Il protocollo fa uso di nonce (*number used once*)
  - numero casuale, impredicibile e inedito il cui scopo è mettere in relazione causale due messaggi
- Tale meccanismo è volto a evitare il riuso doloso di vecchie chiavi di sessione

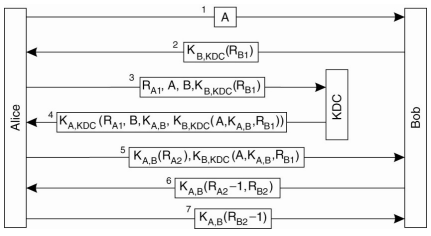
46

Attacco replay

- Un utente malevolo entrato in possesso di una vecchia chiave di sessione può inviare messaggi a Bob fingendosi Alice
  - N.B. Malgrado l'uso dei nonce, lo schema classico soffre questo attacco!

47

Needham-Schroeder rivisitato



48

Kerberos

- Kerberos è un protocollo di autenticazione basato sullo schema Needham-Schroeder rivisitato
  - sviluppato al MIT alla fine degli anni '80
- A quale entità della mitologia si ispira?
  - aspetto chiave: tre teste

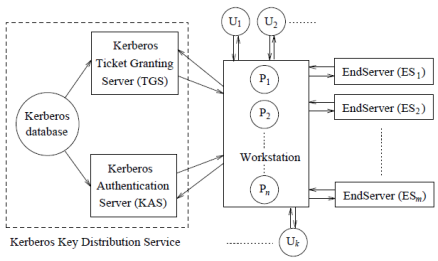
49

Architettura di Kerberos (1)

- L'architettura di Kerberos si basa su tre componenti logiche:
  - processi lanciati dagli utenti
  - server remoti che erogano servizi
  - KDC di Kerberos, composto a sua volta da:
    - TGS (Ticket Granting Service)
    - AS (Authentication Server)

50

Architettura di Kerberos (2)



51

Funzionamento

- Un client ottiene un ticket di lunga durata dall'AS, valido per l'intera sessione di comunicazione
- Quindi, ottiene un ticket di breve durata dal TGS per l'accesso al singolo servizio
- Metafora: il meccanismo è analogo all'abbonamento ai servizi pubblici (carta d'identità/abbonamento a un dato mezzo)

52

Pro e contro

- Garanzia delle proprietà di sicurezza, esclusa l'anonimia
- Garanzia della proprietà di single sign-on: il client non ha necessità di autenticarsi più volte per accedere a servizi diversi
- Nessuna necessità di trasmettere password in rete

- NO anonimia
- Presenza di un singolo punto di fallimento
- La protezione delle password è demandata agli utenti

53

PROBLEMA ATTUALE: LA SICUREZZA NELLE MANET

54

MANET

- Rete wireless caratterizzata da:
  - assenza di infrastruttura fisica fissa
  - topologia dinamica

55

MANET

- Rete wireless caratterizzata da:
  - assenza di infrastruttura fisica fissa
  - topologia dinamica

56

Alcuni scenari applicativi

- Supporto a squadre di soccorso in caso di calamità
- Comunicazioni fra navi durante traversate oceaniche
- Comunicazioni fra satelliti in orbita
- Monitoraggio di fauna in riserve naturali
- Monitoraggio di siti franosi
- Operazioni militari in territorio nemico
- …

57

Protocolli di routing

- Al fine di stabilire comunicazioni fra coppie di nodi, si adottano specifici protocolli di routing
- Tali protocolli si basano sulla cooperazione
  - i nodi intermedi instradano pacchetti
- Ne esistono di tre tipi:
  - proattivi
  - reattivi
  - ibridi

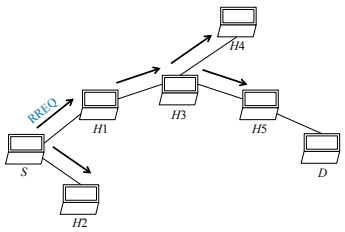
58

AODV

- Uno dei più popolari protocolli per MANET
  - è reattivo
- Pseudocodice dell'algoritmo:
  - If Dest is not in Init's neighborhood and a route to Dest is not in Init's routing table
    - Init broadcasts RREQ packets to its neighbors
  - If a node n receiving the RREQ does not know a way to reach Dest
    - n rebroadcasts the RREQ to its neighbors
  - Otherwise, n unicasts an RREP to Init

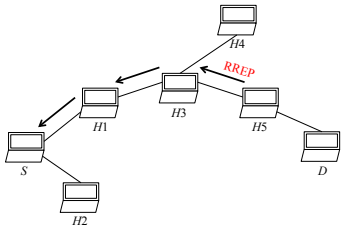
59

Scenario illustrativo (1)



60

Scenario illustrativo (2)



61

Problemi specifici

- Per le loro caratteristiche intrinseche, oltre ai problemi di sicurezza delle reti tradizionali, le MANET soffrono di problemi specifici:
  - le antenne per la trasmissione radio sono omnidirezionali, quindi è impossibile circoscrivere lo spazio di copertura
  - il canale radio dispone di una banda limitata, insufficiente per scambi di grandi moli di dati
  - risorse computazionali e di energia limitate
  - la mobilità causa interferenze, perdite di pacchetti, errori, ritardi

62

Tipologie di attacchi

- Fondamentalmente, esistono due tipologie di attacchi alle MANET:
  - routing disruption: instradano pacchetti fasulli in rete, p.e. attacco blackhole
  - resource consumption: consumano le risorse dei nodi, p.e. attacco DoS

63

Principali meccanismi di protezione

- Le soluzioni a tali attacchi si distinguono in due categorie principali:
  - meccanismi di autenticazione, p.e. crittografia
  - monitoraggio da parte dei nodi del comportamento dei vicini

64

RIFERIMENTI PRINCIPALI

65

- Tanenbaum, A.; Van Steen, M.: «Distributed Systems: Principles and Paradigms», 2nd edition. *Pearson Education* (2007) (chapter 9)
- Rivest, R.; Shamir, A.; Adleman, L.: «A Method for Obtaining Digital Signatures and Public-Key Cryptosystems». *Communications of the ACM*, 21(2), pp. 120-126 (1978)
- Needham, R.; Schroeder, M.: «Using encryption for authentication in large networks of computers». *Communications of the ACM*, 21(12), pp. 993-999 (1978)
- http://web.mit.edu/kerberos/
- Kannhavong, B.; Nakayama, H.; Nemoto, Y.; Kato, N.; Jamalipour, A.: «A Survey of Routing Attacks in Mobile Ad Hoc Networks». *IEEE Wireless Communications*, 14(5), pp. 85-91 (2007)

66