Lezione del 27 Maggio 2016

ACL estese e D.H.

REGOLE ACL ESTESE)

37

SINTASSI GENERALE

ACCESS-LIST # {PERMIT | DENY} PROTOCOLLO SOURCE MASK

DESTINATION MASK OPERATORE OPERANDO

CAMPI:

PROTOCOLLO: IP, TCP, UDP, ICMP, ECC...

SOURCE, DESTINATION: INDIRIZZI SORG. & DEST.

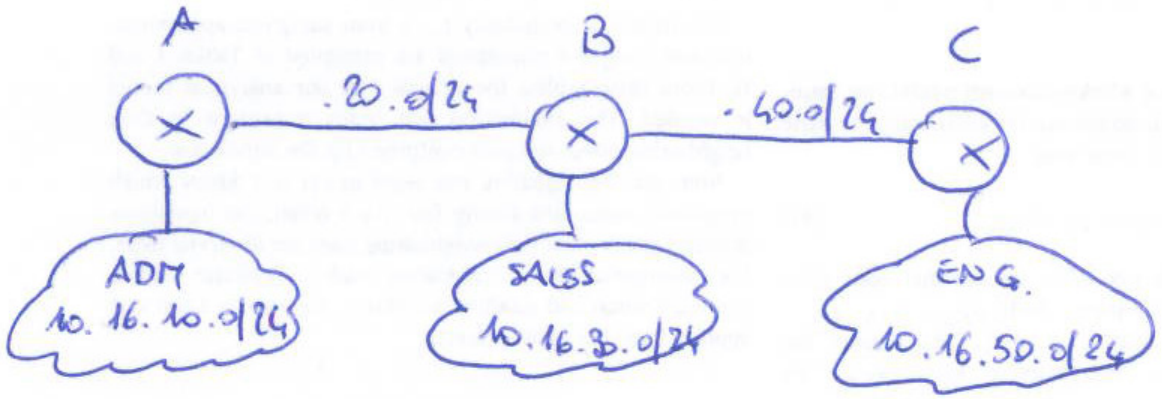
MASK: WILDCARD DI SORGENTE & DESTINAZIONE

OPERATORE: LESS THAN, GREATER THAN, EQUAL, NOT EQUAL, ECC...

OPERANDO: GENERALMENTE È UNA PORTA

#: PER LE ACL STANDARD SI USANO VALORI DA 1:99, PER LE ESTESE DA 100 A 199

ES.)



SI VUOLE CHE IL ROUTER A PERMETTA SOLO ALL'HOST DI EN 10.16.50.2 DI ACCEDERE ALL'HOST 10.16.10.2 DI ADM, SU LA PORTA 80 TCP

RA
ACCESS-LIST 118 PERMIT TCP HOST 10.16.50.2 HOST 10.16.10.2 EQ 80

ASSIGN 118 IF 10.16.10.1 OUT

UNA POSSIBILE SOLUZIONE

RSA (RIVEST - SHAMIR - ADLEMAN) 1978

RICERCATORI MIT

BASATO SULLE OSSERVAZIONI DI DIFFIE ED HELLMAN SULLA CODIFICA ASIMMETRICA. DH INTRODUSSERO L'IDEA, MENTRE RSA SFRUTTARONO APPLICANDO PRINCIPI MATEMATICI DI NUMERI PRIMI CON MOLTE CIFRE.

NEL 2005, IN 5 MESI SI RIUSCÌ A DECIFRARE UN MESSAGGIO RSA-640, UTILIZZANDO UN SUPERCOMPUTER DA 2.2 GHz.

IN GENERALE SI PUÒ USARE PER CODIFICARE UN MSG CONTENENTE UNA CHIAVE SEGRETA, USATA IN SEGUITO PER CODIFICA SIMMETRICA

PARTIAMO DALL'ALGORITMO DH

SIA DATO UN GENERATORE (g) (DETTO ANCHE BASE) E (p) NUMERO PRIMO.

(g, p) ≡ CHIAVE PUBBLICA

L'UTENTE 1 SCEGLIE UN NUMERO CASUALE a E CALCOLA $A = g^a \bmod p$

(CHIAVE PRIVATA DI UT. 1)

L'UTENTE 1 COMUNICA ALL'UTENTE 2 g, p, A.
(CHIAVE PRIVATA DI UT. 2)

L'UTENTE 2 SCEGLIE UN NUMERO CASUALE b E CALCOLA $B = g^b \bmod p$

INVIANDO B ALL'UTENTE 1.

CALCOLATI IN PRIVATO

UT. 1 CALCOLA $K_A = B^a \bmod p$ E UT. 2 CALCOLA $K_B = A^b \bmod p$

MA $K_A = K_B$ IN QUANTO $B^a \bmod p = A^b \bmod p \iff B^a = A^b$

$$B^a = g^{ba} \quad e \quad A^b = g^{ab} \Rightarrow g^{ba} = g^{ab}$$

IL MALINTENZIONATO POTREBBE CONOSCERE g, p, A e B, MA DOVREBBE INVERTIRE L'OP. DI POTENZA (CON LOGARITMO). CONSIDERANDO a e b SONO COMPOSTI DA ALMENO 100 CIFRE E p È UN NUMERO PRIMO DI ALMENO 300 CIFRE. È NON DEVE ESSERE GRANDE (GENERALMENTE VALE 2 o 5)

È RESISTENTE AGLI ATTACCHI SNIFFING ("ASCOLTARE" I VALORI (28
3 FARE I CALCOLI IN PROPRIO) MA È SENSIBILE AL MAN-IN-THE-MIDDLE,
DATO CHE IL MALINTENZIONATO RIESCE FACILMENTE I VALORI
SCAMBIATI TRA GLI INTERLOCUTORI

ES.

DATI PUBBLICI : BASE $g = 5$, $p = 41$,

DATI PRIVATI : UT. 1 $a = 12$

UT. 2 $b = 25$

ILLUSTRARE LO SCAMBIO DI MSG PREVISTI DALL'APPROCCIO DH:

1) UT. 1 CALCOLA $A = g^a \bmod p = 5^{12} \bmod 41 = 244140625 \bmod 41 = 16$

UT. 1 INVIA $A = 16$ ALL'UT. 2

2) UT. 2 CALCOLA $B = g^b \bmod p = 5^{25} \bmod 41 = 29802322388... \bmod 41 = 9$

UT. 2 INVIA $B = 9$ ALL'UT. 1

3) CALCOLO CHIAVE UT. 1 $K_A = B^a \bmod p = 9^{12} \bmod 41 = 1$

UT. 2 $K_B = A^b \bmod p = 16^{25} \bmod 41 = 1$