Corso di Sicurezza A.A.2017-2018

ESONERO 1 -- aprile 2018

Le soluzioni devono essere ricevute in formato pdf entro le 22 di martedì 1 maggio 2018.

La prima pagina delle soluzioni sottomesse deve riportare, in aggiunta al Nome, Cognome e numero di matricola, la seguente dichiarazione:
"Dichiaro di aver completato questo esonero da solo/a e di non aver discusso le soluzioni con altri studenti in classe."

PROBLEMA 1 [3+3+4 punti]
Vogliamo simulare il modello Take-Grant in HRU, ed in particolare i comandi di *take* e di *grant*.

a) implementare con la sintassi di HRU il comando *take(primo, secondo, obj, right)* con il quale il soggetto *primo* prende il permesso *righ*t su *obj* dal soggetto *secondo*
b) implementare con la sintassi di HRU il comando *grant(primo, secondo, obj, right)* con il quale il soggetto *primo* da il permesso *right* su *obj* al soggetto *secondo*
c) Con riferimento solo ai due comandi appena implementati, è la safety del sistema ottenuto decidibile? Perché?

PROBLEMA 2 [3 x 5 punti]
Un blocco di plaintext di 576 bit è criptato con DES con una delle modalità di cifratura producendo un blocco di ciphertext di 576 bit.. Il ciphertext viene spedito al ricevente per essere decifrato. Durante la trasmissione, il bit 182 viene scambiato.
Quali bit POTREBBERO essere sbagliati dopo la decifratura usando CBC?
Quali bit POTREBBERO essere sbagliati dopo la decifratura usando CFB nella versione con fasi di cifratura di 32 bit (32 bit sono criptati ad ogni turno)?
Quali bit POTREBBERO essere sbagliati dopo la decifratura usando OFB nella versione con fasi di cifratura di 32 bit (32 bit sono criptati ad ogni turno)?
SPIEGARE !!

PROBLEMA 3 [5 x 3 punti]
Quali delle cinque modalità di cifratura a blocchi (ECB, CBC, CFB, OFB, CTR) possono essere usate **con efficacia** (non facilmente compromesse) utilizzando un sistema a chiave pubblica tipo RSA invece di DES o AES ? **SPIEGARE !**

PROBLEMA 4 [5+10 punti]
Perché è indispensabile che una CRL (Certificate Revocation List) sia rinnovata periodicamente, anche se non ci sono nuovi certificati revocati da aggiungere alla lista?
Quale/i principio/i di Secure Design viene/vengono violati con l'utilizzo dei CRL? Perché?

PROBLEMA 5 [2 x 5 punti]

Ci sono 3 proprietà desiderabili di una funzione hash crittografica:

1. resistente alla pre-immagine [data y, trovare x tale che f(x)=y] ,
2. resistente ad altra pre-immagine [dati x,y con y=f(x), trovare altra x' tale che f(x')=y], e
3. resistente alle collisioni [trovare x e x' tali che f(x)=f(x')].

Per ciascuna delle applicazioni seguenti, spiegare quale/i proprietà è/sono necessaria/e e quale/i no.

a) Attilio propone a Beatrice un problema difficile che dichiara di saper risolvere. Beatrice vuole provare a risolverlo, ma vuole anche essere sicura che Attilio non stia bleffando. Quindi Attilio scrive la propria soluzione, appende alcuni bit randomici, calcola il valore hash e manda a Beatrice il valore finale (soluzione e bit randomici rimangono segreti). Quando Beatrice trova la soluzione, Attilio può verificare la correttezza della soluzione di Beatrice priva di rivelare la sua soluzione (ed i bit randomici) che lui aveva inviato prima.

b) Un amministratore di sistema, preoccupato di possibili intromissioni, calcola il valore hash di file binari importanti e conserva i valori hash in un file read-only. Un programma ricalcola periodicamente i valori hash dei file che contengono i binari e li confronta con i valori conservati. Un utente malizioso che riuscisse a sovrascrivere uno dei file protetti non dovrebbe essere in grado di cambiarli senza essere scoperto.

PROBLEMA 6 [10 punti]

Un esperto di Informatica dichiara di avere sviluppato un programma `CHECK` che stabilisce se un certo frammento di software è un virus oppure no (cioè, dato un programma P, `CHECK(P)` restituisce **true** se P è un virus o **false** altrimenti).
Supponiamo di avere a disposizione una procedura `infect_executable` che, quando invocata, esamina la memoria alla ricerca di file eseguibili e si copia all'interno di questi programmi.
Vi viene fornito un programma `CONTROL` che contiene al suo interno il seguente frammento, unica occorrenza nel programma `CONTROL` della chiamata a `infect_executable`

```
{
    …
    if CHECK(CONTROL) then EXIT() else infect_executable ;
    …
}
```

Stabilire (e **SPIEGARE**) se `CHECK` decide correttamente se `CONTROL` è un virus oppure no.

PROBLEMA 7 [5+5 punti]

Un esperto (?) di sicurezza propone il seguente protocollo per permettere ad un cliente C di autenticarsi presso un server S utilizzando un servizio di autenticazione AUT (chiave condivisa da X e Y indicate con $K_{X,Y}$)

C -> S	C	(C manda ad S il messaggio "C")
S -> C	N	(S risponde a C con il messaggio "N(once)")
C -> S	$K_{C,AUT}$ [N]	
S -> AUT	$K_{S,AUT}$ [C , $K_{C,AUT}$[N]]	
AUT -> S	$K_{S,AUT}$ [N]	

Spiegare perché il protocollo non è sicuro e proporre una modifica al protocollo per rimuovere il problema.